S. HRG. 115–683

FACEBOOK, SOCIAL MEDIA PRIVACY, AND THE USE AND ABUSE OF DATA

JOINT HEARING

BEFORE THE

COMMITTEE ON COMMERCE, SCIENCE, AND TRANSPORTATION UNITED STATES SENATE

AND THE

COMMITTEE ON THE JUDICIARY UNITED STATES SENATE

ONE HUNDRED FIFTEENTH CONGRESS

SECOND SESSION

APRIL 10, 2018

Serial No. J–115–40

Printed for the use of the Committee on Commerce, Science, and Transportation

Available online: http://www.govinfo.gov

FACEBOOK, SOCIAL MEDIA PRIVACY, AND THE USE AND ABUSE OF DATA

S. HRG. 115–683

FACEBOOK, SOCIAL MEDIA PRIVACY, AND THE USE AND ABUSE OF DATA

JOINT HEARING

BEFORE THE

COMMITTEE ON COMMERCE, SCIENCE, AND TRANSPORTATION UNITED STATES SENATE

AND THE

COMMITTEE ON THE JUDICIARY UNITED STATES SENATE

ONE HUNDRED FIFTEENTH CONGRESS

SECOND SESSION

APRIL 10, 2018

Serial No. J–115–40

Printed for the use of the Committee on Commerce, Science, and Transportation

Available online: http://www.govinfo.gov

U.S. GOVERNMENT PUBLISHING OFFICE

37–801 PDF WASHINGTON : 2019

SENATE COMMITTEE ON COMMERCE, SCIENCE, AND TRANSPORTATION

ONE HUNDRED FIFTEENTH CONGRESS

SECOND SESSION

JOHN THUNE, South Dakota, *Chairman*

ROGER WICKER, Mississippi
ROY BLUNT, Missouri
TED CRUZ, Texas
DEB FISCHER, Nebraska
JERRY MORAN, Kansas
DAN SULLIVAN, Alaska
DEAN HELLER, Nevada
JAMES INHOFE, Oklahoma
MIKE LEE, Utah
RON JOHNSON, Wisconsin
SHELLEY MOORE CAPITO, West Virginia
CORY GARDNER, Colorado
TODD YOUNG, Indiana

BILL NELSON, Florida, *Ranking*
MARIA CANTWELL, Washington
AMY KLOBUCHAR, Minnesota
RICHARD BLUMENTHAL, Connecticut
BRIAN SCHATZ, Hawaii
EDWARD MARKEY, Massachusetts
TOM UDALL, New Mexico
GARY PETERS, Michigan
TAMMY BALDWIN, Wisconsin
TAMMY DUCKWORTH, Illinois
MAGGIE HASSAN, New Hampshire
CATHERINE CORTEZ MASTO, Nevada
JON TESTER, Montana

NICK ROSSI, *Staff Director*
ADRIAN ARNAKIS, *Deputy Staff Director*
JASON VAN BEEK, *General Counsel*
KIM LIPSKY, *Democratic Staff Director*
CHRIS DAY, *Democratic Deputy Staff Director*
RENAE BLACK, *Senior Counsel*

SENATE COMMITTEE ON THE JUDICIARY

ONE HUNDRED FIFTEENTH CONGRESS

SECOND SESSION

CHUCK GRASSLEY, Iowa, *Chairman*

ORRIN HATCH, Utah
LINDSEY GRAHAM, South Carolina
JOHN CORNYN, Texas
MIKE LEE, Utah
TED CRUZ, Texas
BEN SASSE, Nebraska
JEFF FLAKE, Arizona
MIKE CRAPO, Idaho
THOM TILLIS, North Carolina
JOHN KENNEDY, Louisiana

DIANNE FEINSTEIN, California, *Ranking*
PATRICK LEAHY, Vermont
RICHARD DURBIN, Illinois
SHELDON WHITEHOUSE, Rhode Island
AMY KLOBUCHAR, Minnesota
CHRISTOPHER COONS, Delaware
RICHARD BLUMENTHAL, Connecticut
MAZIE HIRONO, Hawaii
CORY BOOKER, New Jeresey
KAMALA HARRIS, California

CONTENTS

FACEBOOK, SOCIAL MEDIA PRIVACY, AND THE USE AND ABUSE OF DATA

TUESDAY, APRIL 10, 2018

U.S. SENATE,
COMMITTEE ON COMMERCE, SCIENCE, AND TRANSPORTATION,
AND COMMITTEE ON THE JUDICIARY,
Washington, DC.

The Committees met, pursuant to notice, at 2:30 p.m., in room 216, Hart Senate Office Building, Hon. Chuck Grassley, Chairman of the Committee on the Judiciary, presiding.

Present from the Committee on Commerce, Science, and Transportation: Senators Thune, Wicker, Blunt, Cruz, Fischer, Moran, Sullivan, Heller, Inhofe, Johnson, Capito, Gardner, Young, Nelson, Cantwell, Klobuchar, Blumenthal, Schatz, Markey, Udall, Peters, Baldwin, Hassan, Cortez Masto, and Tester.

Present from the Committee on the Judiciary: Senators Grassley [presiding], Hatch, Graham, Cornyn, Cruz, Lee, Sasse, Flake, Crapo, Tillis, Kennedy, Feinstein, Leahy, Durbin, Whitehouse, Klobuchar, Coons, Blumenthal, Hirono, Booker, and Harris.

OPENING STATEMENT OF HON. CHUCK GRASSLEY, U.S. SENATOR FROM IOWA

Chairman GRASSLEY. The committees on the Judiciary and Commerce, Science, and Transportation will come to order.

We welcome everyone to today's hearing on "Facebook, Social Media Privacy, and the Use and Abuse of Data." Although not unprecedented, this is a unique hearing. The issues we will consider range from data privacy and security to consumer protection and the Federal Trade Commission enforcement, touching on jurisdictions of these two committees.

We have 44 members between our two committees. That may not seem like a large group by Facebook standards, but it is significant here for a hearing in the United States Senate. We will do our best to keep things moving efficiently, given our circumstances.

We will begin with opening statements from the chairmen and ranking members of each committee, starting with Chairman Thune, and then proceed with Mr. Zuckerberg's opening statement. We will then move on to questioning. Each member will have 5 minutes to question witnesses.

I would like to remind the members of both committees that time limits will be and must be strictly enforced given the numbers that we have here today. If you are over your time, Chairman Thune and I will make sure to let you know. There will not be a second round as well. Of course, there will be the usual follow-up written

questions through the record. Questioning will alternate between majority and minority and between committees. We will proceed in order based on respective committee seniority.

We will anticipate a couple short breaks later in the afternoon, and so it is my pleasure to recognize the Chairman of the Commerce Committee, Chairman Thune, for his opening statement.

STATEMENT OF HON. JOHN THUNE,
U.S. SENATOR FROM SOUTH DAKOTA

Chairman THUNE. Thank you, Chairman Grassley.

Today's hearing is extraordinary. It is extraordinary to hold a joint committee hearing. It is even more extraordinary to have a single CEO testify before nearly half of the U.S. Senate. But then Facebook is pretty extraordinary. More than 2 billion people use Facebook every month. One point four billion people use it every day, more than the population of any country on Earth except China and more than four times the population of the United States. It is also more than 1,500 times the population of my home state of South Dakota. Plus, roughly 45 percent of American adults report getting at least some of their news from Facebook.

In many respects, Facebook's incredible reach is why we are here today. We are here because of what you, Mr. Zuckerberg, have described as a breach of trust. A quiz app used by approximately 300,000 people led to information about 87 million Facebook users being obtained by the company Cambridge Analytica. There are plenty of questions about the behavior of Cambridge Analytica, and we expect to hold a future hearing on Cambridge and similar firms.

But as you have said, this is not likely to be an isolated incident, a fact demonstrated by Facebook's suspension of another firm just this past weekend. You have promised that when Facebook discovers other apps that access to large amounts of user data, you will ban them and tell those affected. And that is appropriate. But it is unlikely to be enough for the 2 billion Facebook users.

One reason that so many people are worried about this incident is what it says about how Facebook works. The idea that for every person who decided to try an app, information about nearly 300 other people was scraped from your services, to put it mildly, disturbing. And the fact that those 87 million people may have technically consented to making their data available does not make most people feel any better.

The recent revelation that malicious actors were able to utilize Facebook's default privacy settings to match e-mail addresses and phone numbers found on the so-called dark web to public Facebook profiles, potentially affecting all Facebook users, only adds fuel to the fire.

What binds these two incidents is that they do not appear to be caused by the kind of negligence that allows typical data breaches to happen. Instead, they both appear to be the result of people exploiting the very tools that you have created to manipulate users' information.

I know Facebook has taken several steps and intends to take more to address these issues. Nevertheless, some have warned that the actions Facebook is taking to ensure that third parties do not obtain data from unsuspecting users, while necessary, will actually

serve to enhance Facebook's own ability to market such data exclusively.

Most of us understand that, whether you are using Facebook or Google or some other online services, we are trading certain information about ourselves for free or low-cost services. But for this model to persist, both sides of the bargain need to know the stakes that are involved. Right now, I am not convinced that Facebook users have the information that they need to make meaningful choices.

In the past, many of my colleagues on both sides of the aisle have been willing to defer to tech companies' efforts to regulate themselves, but this may be changing. Just last month, in overwhelming bipartisan fashion, Congress voted to make it easier for prosecutors and victims to go after websites that knowingly facilitate sex trafficking. This should be a wake-up call for the tech community. We want to hear more without delay about what Facebook and other companies plan to do to take greater responsibility for what happens on their platforms. How will you protect users' data? How will you inform users about the changes that you are making? And how do you intend to proactively stop harmful conduct instead of being forced to respond to it months or years later?

Mr. Zuckerberg, in many ways, you and the company that you have created, the story that you have created represent the American dream. Many are incredibly inspired by what you have done. At the same time, you have an obligation and it is up to you to ensure that that dream does not become a privacy nightmare for the scores of people who use Facebook.

This hearing is an opportunity to speak to those who believe in Facebook and to those who are deeply skeptical about it. We are listening, America is listening, and quite possibly, the world is listening, too.

Chairman GRASSLEY. Thank you. And now, Ranking Member Feinstein.

STATEMENT OF HON. DIANNE FEINSTEIN,
U.S. SENATOR FROM CALIFORNIA

Senator FEINSTEIN. Thank you very much, Mr. Chairman. Chairman Grassley, Chairman Thune, thank you both for holding this hearing.

Mr. Zuckerberg, thank you for being here. You have a real opportunity this afternoon to lead the industry and demonstrate a meaningful commitment to protecting individual privacy.

We have learned over the past few months, and we have learned a great deal that is alarming. We have seen how foreign actors are abusing social media platforms like Facebook to interfere in elections and take millions of Americans' personal information without their knowledge in order to manipulate public opinion and target individual voters.

Specifically, on February 16, Special Counsel Mueller issued an indictment against the Russia-based Internet Research Agency and 13 of its employees for interfering with operations targeting the United States. Through this 37-page indictment, we learned that the IRA ran a coordinated campaign through 470 Facebook accounts and pages. The campaign included ads and false information

to create discord and harm Secretary Clinton's campaign. And the content was seen by an estimated 157 million Americans.

A month later, on March 17, news broke that Cambridge Analytica exploited the personal information of approximately 50 million Facebook users without their knowledge or permission. And last week, we learned that number was even higher, 87 million Facebook users who had their private information taken without their consent. Specifically, using a personality quiz he created, Professor Kogan collected the personal information of 300,000 Facebook users and then collected data on millions of their friends. It appears the information collected included everything these individuals had on their Facebook pages and, according to some reports, even included private direct messages between users.

Professor Kogan is said to have taken data from over 70 million Americans. It has also been reported that he sold this data to Cambridge Analytica for $800,000. Cambridge Analytica then took this data and created a psychological welfare tool to influence United States elections. In fact, the CEO Alexander Nix declared that Cambridge Analytica ran all the digital campaign, the television campaign, and its data informed all the strategy for the Trump campaign. The reporting has also speculated that Cambridge Analytica worked with the Internet Research Agency to help Russia identify which American voters to target with its propaganda.

I am concerned that press reports indicate Facebook learned about this breach in 2015 but appears not to have taken significant steps to address it until this year.

So this hearing is important, and I appreciate the conversation we had yesterday. And I believe that Facebook, through your presence here today and the words you are about to tell us, will indicate how strongly your industry will regulate and/or reform the platforms that they control. I believe this is extraordinarily important. You lead a big company with 27,000 employees, and we very much look forward to your comments.

Thank you, Mr. Chairman.

Chairman GRASSLEY. Thank you, Senator Feinstein.

The history and growth of Facebook mirrors that of many of our technological giants. Founded by Mr. Zuckerberg in 2004, Facebook has exploded over the past 14 years. Facebook currently has over 2.13 billion monthly active users across the world, over than 25,000 employees, and offices in 13 U.S. cities and various other countries.

Like their expanding user base, the data collected on Facebook users has also skyrocketed. They have moved on from schools, likes, and relationship statuses. Today, Facebook has access to dozens of data points, ranging from ads that you have clicked on, events you have attended, and your location based upon your mobile device.

It is no secret that Facebook makes money off this data through advertising revenue, although many seem confused by, or altogether unaware, of this fact. Facebook generated $40 billion in revenue in 2017, with about 98 percent coming from advertising across Facebook and Instagram.

Significant data collection is also occurring at Google, Twitter, Apple, and Amazon. An ever-expanding portfolio of products and services offered by these companies grant endless opportunities to

collect increasing amounts of information on their customers. As we get more free or extremely low-cost services, the tradeoff for the American consumer is to provide more personal data. The potential for further growth and innovation based on collection of data is limitless. However, the potential for abuse is also significant.

While the contours of the Cambridge Analytica situation are still coming to light, there was clearly a breach of consumer trust and a likely improper transfer of data. The Judiciary Committee will hold a separate hearing exploring Cambridge and other data privacy issues. More importantly though, these events have ignited a larger discussion on consumers' expectations and the future of data privacy in our society. It has exposed that consumers may not fully understand or appreciate the extent to which their data is collected, protected, transferred, used, and misused.

Data has been used in advertising and political campaigns for decades. The amount and type of data obtained, however, has seen a very dramatic change. Campaigns, including Presidents Bush, Obama, and Trump, all used these increasing amounts of data to focus on micro-targeting and personalization over numerous social media platforms, and especially Facebook.

In fact, President Obama's campaign developed an app utilizing the same Facebook feature as Cambridge Analytica to capture the information of not just the apps users, but millions of their friends. The digital director for that campaign for 2012 described the data-scraping app as something that would, "wind up being the most groundbreaking piece of technology developed for this campaign."

So the effectiveness of these social media tactics can be debated, but their use over the past years across the political spectrum and their increased significance cannot be ignored. Our policy toward data privacy and security must keep pace with these changes. Data privacy should be tethered to consumer needs and expectations.

Now, at a minimum, consumers must have the transparency necessary to make an informed decision about whether to share their data and how it can be used. Consumers ought to have clear information, not opaque policies and complex click-through consent pages. The tech industry has an obligation to respond to widespread and growing concerns over data privacy and security and to restore the public's trust. The status quo no longer works.

Moreover, Congress must determine if and how we need to strengthen privacy standards to ensure transparency and understanding for the billions of consumers who utilize these products.

[The prepared statement of Chairman Grassley follows:]

PREPARED STATEMENT OF HON. CHUCK GRASSLEY, U.S. SENATOR FROM IOWA

The history and growth of Facebook mirrors that of many of our technology giants. Founded by Mr. Zuckerberg in 2004, Facebook has exploded over the last 14 years. Facebook currently has 2.13 billion monthly active users across the world, more than 25,000 employees, and offices in 13 U.S. cities and various other countries.

Like their expanding user base, the data collected on Facebook users has also skyrocketed. They have moved on from schools, likes, and relationship status. Today, Facebook has access to dozens of data points, ranging from ads you've clicked on, events you've attended, and your location based on your mobile device.

It is no secret that Facebook makes money off this data through advertising revenue, although many seem confused by, or altogether unaware, of this fact.

Facebook generated $40 billion in revenue in 2017, with about 98 percent coming from advertising across Facebook and Instagram.

Significant data collection is also occurring at Google, Twitter, Apple, and Amazon. An ever-expanding portfolio of products and services offered by these companies grant endless opportunities to collect increasing amounts of information on their customers. As we get more free, or extremely low-cost, services, the tradeoff for the American consumer is to provide more personal data.

The potential for further growth and innovation based on the collection of data is limitless. However, the potential for abuse is significant.

While the contours of the Cambridge Analytica situation are still coming to light, there was clearly a breach of consumer trust and a likely improper transfer of data. The Judiciary Committee will hold a separate hearing exploring Cambridge and other data privacy issues.

More importantly though, these events have ignited a larger discussion on consumers' expectations and the future of data privacy in our society.

It has exposed that consumers may not fully understand or appreciate the extent to which their data is collected, protected, transferred, used and misused.

Data has been used in advertising and political campaigns for decades. The amount and types of data obtained, however, has seen a dramatic change. Campaigns, including President Bush, Obama, and Trump, all used these increasing amounts of data to focus on micro-targeting and personalization over numerous social media platforms, especially Facebook.

In fact, President Obama's campaign developed an app utilizing the same Facebook feature as Cambridge Analytica to capture the information of not just the apps users, but millions of their friends. The digital director for Obama for America 2012 described the data-scraping app as something that would "wind up being the most groundbreaking piece of technology developed for this campaign".

The effectiveness of these social media tactics can be debated, but their use over the past years across the political spectrum and their increased significance cannot.

Our policy towards data privacy and security must keep pace with these changes. Data privacy should be tethered to consumer needs and expectations.

At a minimum, consumers must have the transparency necessary to make informed decisions about whether to share their data and how it can be used. Consumers ought to have clear information, not opaque policies and complex click-through consent pages.

The tech industry has an obligation to respond to widespread and growing concerns over data privacy and security and to restore the public trust. The status quo no longer works.

Moreover, Congress must determine if and how we need to strengthen privacy standards to ensure transparency and understanding for the billions of consumers who utilize these products.

Chairman GRASSLEY. Senator Nelson.

STATEMENT OF HON. BILL NELSON, U.S. SENATOR FROM FLORIDA

Senator NELSON. Thank you, Mr. Chairman.

Mr. Zuckerberg, good afternoon.

Let me just cut to the chase. If you and other social media companies do not get your act in order, none of us are going to have any privacy anymore. That is what we are facing. We are talking about personally identifiable information that, if not kept by the social media companies from theft, we will not have our personal privacy anymore, a value that we have in America.

It is the advent of technology, and of course all of us are part of it. From the moment that we wake up in the morning until we go to bed, we are on those handheld tablets, and online companies like Facebook are tracking our activities and collecting information. Facebook has a responsibility to protect this personal information.

We had a good discussion yesterday. We went over all of this. You told me that the company had failed to protect privacy. It is not the first time that Facebook has mishandled its users' informa-

tion. The FTC found that Facebook's privacy policies had deceived users in the past. And in the present case, we recognize that Cambridge Analytica and an app developer lied to consumers and lied to you, lied to Facebook, but did Facebook watch over the operations? We want to know that. And why did Facebook not notify 87 million users that their personally identifiable information had been taken? And why were they not informed that it was also being used for unauthorized political purposes?

So only now—and I appreciate our conversation. Only now, Facebook has pledged to inform those consumers whose accounts were compromised. I think you are genuine. I got that sense in conversing with you. You want to do the right thing. You want to enact reforms. We want to know if it is going to be enough. And I hope that will be in the answers today.

Now, since we still do not know what Cambridge Analytica has done with this data, you heard Chairman Thune say, as we have discussed, we want to haul Cambridge Analytica in to answer these questions at a separate hearing.

I want to thank Chairman Thune for working with all of us on scheduling a hearing. There is obviously a great deal of interest in this subject. I hope we can get to the bottom of this. And if Facebook and other online companies will not or cannot fix the privacy invasions, then we are going to have to, we, the Congress. How can American consumers trust folks like your company to be caretakers of their most personal and identifiable information? And that is the question. Thank you.

[The prepared statement of Senator Nelson follows:]

PREPARED STATEMENT OF HON. BILL NELSON, U.S. SENATOR FROM FLORIDA

Let me get to the point, one that I made to Mr. Zuckerberg yesterday during our lengthy conversation in my office. If Facebook and other social media and online companies don't do a better job as stewards of our personal information, American consumers are no longer going to have any privacy to protect.

From the minute consumers wake up to the minute they put down their smartphone at the end of the day, online companies like Facebook are tracking their activities and collecting information. Facebook has a responsibility to protect this personal information.

Unfortunately, I believe that the company failed to do so. This is not the first time that Facebook has mishandled its users' information. The Federal Trade Commission found that Facebook's privacy policies had deceived users in the past.

In the present case, I recognize that Cambridge Analytica and an app developer lied to consumers and lied to Facebook. But did Facebook watch over their operations? And why didn't Facebook notify eighty-seven million users when it discovered that Cambridge Analytica had inappropriately gotten hold of their sensitive information and was using it for unauthorized political purposes?

Only now has Facebook pledged to inform those consumers whose accounts were compromised. I know Mr. Zuckerberg wants to do the right thing and enact reforms, but will it be enough? I hope to get some answers today.

Lastly, we still don't know exactly what Cambridge Analytica has done with this data. That's why I have asked Chairman Thune to haul Cambridge Analytica in to answer these questions at a separate hearing. I want to thank the chairman for working with me on scheduling a hearing in the near future.

There is obviously a great deal of interest in this subject, and I hope that we can get to the bottom line. That is, if Facebook and other online companies will not or cannot fix these privacy invasions, then we will. How can American consumers trust them to be caretakers of their most personal and identifiable information?

Chairman GRASSLEY. Thank you, my colleagues, and Senator Nelson.

Our witness today is Mark Zuckerberg, Founder, Chairman, Chief Executive Officer of Facebook. Mr. Zuckerberg launched Facebook February 4, 2004, at the age of 19. And at that time he was a student at Harvard University. As I mentioned previously, his company now has over $40 billion of annual revenue and over 2 billion monthly active users. Mr. Zuckerberg, along with his wife, also established the Chan Zuckerberg Initiative to further philanthropic causes.

I now turn to you. Welcome to the Committee. And whatever your statement is orally, if you have a longer one, it will be included in the record. So, proceed, sir.

STATEMENT OF MARK ZUCKERBERG, CHAIRMAN AND CHIEF EXECUTIVE OFFICER, FACEBOOK

Mr. ZUCKERBERG. Chairman Grassley, Chairman Thune, Ranking Member Feinstein, and Ranking Member Nelson and members of the Committee, we face a number of important issues around privacy, safety, and democracy, and you will rightfully have some hard questions for me to answer. Before I talk about the steps we are taking to address them, I want to talk about how we got here.

Facebook is an idealistic and optimistic company. For most of our existence, we focused on all of the good that connecting people can do. And as Facebook has grown, people everywhere have gotten a powerful new tool for staying connected to the people they love, for making their voices heard, and for building communities and businesses. Just recently, we have seen the #metoo movement and the March for Our Lives organized, at least in part, on Facebook. After Hurricane Harvey, people came together to raise more than $20 million for relief. And more than 70 million small businesses use Facebook to create jobs and grow.

But it is clear now that we did not do enough to prevent these tools for being used for harm as well, and that goes for fake news, for foreign interference in elections, and hate speech, as well as developers and data privacy. We did not take a broad enough view of our responsibility, and that was a big mistake. And it was my mistake, and I am sorry. I started Facebook, I run it, and I am responsible for what happens here.

So now, we have to go through all of our relationship with people and make sure that we are taking a broad enough view of our responsibility. It is not enough to just connect people; we have to make sure that those connections are positive. It is not enough to just give people a voice; we need to make sure that people are not using it to harm other people or to spread misinformation. And it is not enough to just give people control over their information; we need to make sure that the developers they share it with protect their information, too. Across the board, we have a responsibility to not just build tools but to make sure that they are used for good.

It will take some time to work through all the changes we need to make across the company, but I am committed to getting this right. This includes the basic responsibility of protecting people's information, which we failed to do with Cambridge Analytica. So here are a few things that we are doing to address this and to prevent it from happening again.

First, we are getting to the bottom of exactly what Cambridge Analytica did and telling everyone affected. What we know now is that Cambridge Analytica improperly accessed some information about millions of Facebook members by buying it from an app developer. This was information that people generally shared publicly on their Facebook pages like names and their profile picture and the pages they follow.

When we first contacted Cambridge Analytica, they told us that they had deleted the data. About a month ago, we heard new reports that suggested that was not true. And now, we are working with governments in the U.S., the U.K., and around the world to do a full audit of what they have done and to make sure that they get rid of any data they may still have.

Second, to make sure no other app developers out there are misusing data, we are now investigating every single app that had access to a large amount of information in the past. And if we find that someone improperly used data, we are going to ban them from Facebook and tell everyone affected.

Third, to prevent this from ever happening again going forward, we are making sure that developers cannot access as much information now. The good news here is that we already made big changes to our platform in 2014 that would have prevented this specific situation with Cambridge Analytica from occurring again today. But there is more to do, and you can find more details on the steps we are taking in my written statement.

My top priority has always been our social mission of connecting people, building community, and bringing the world closer together. Advertisers and developers will never take priority over that as long as I am running Facebook.

I started Facebook when I was in college. We have come a long way since then. We now serve more than 2 billion people around the world, and every day, people use our services to stay connected with the people that matter to them most. I believe deeply in what we are doing, and I know that when we address these challenges, we will look back and view helping people connect and giving more people a voice is a positive force in the world.

I realize the issues we are talking about today are not just issues for Facebook and our community; they are issues and challenges for all of us as Americans.

Thank you for having me here today, and I am ready to take your questions.

[The prepared statement of Mr. Zuckerberg follows:]

PREPARED STATEMENT OF MARK ZUCKERBERG, CHAIRMAN AND CHIEF EXECUTIVE OFFICER, FACEBOOK

I. Introduction

Chairman Grassley, Chairman Thune, Ranking Member Feinstein, Ranking Member Nelson, and Members of the Committees,

We face a number of important issues around privacy, safety, and democracy, and you will rightfully have some hard questions for me to answer. Before I talk about the steps we're taking to address them, I want to talk about how we got here.

Facebook is an idealistic and optimistic company. For most of our existence, we focused on all the good that connecting people can bring. As Facebook has grown, people everywhere have gotten a powerful new tool to stay connected to the people they love, make their voices heard, and build communities and businesses. Just re-

cently, we've seen the #metoo movement and the March for Our Lives, organized, at least in part, on Facebook. After Hurricane Harvey, people raised more than $20 million for relief. And more than 70 million small businesses now use Facebook to grow and create jobs.

But it's clear now that we didn't do enough to prevent these tools from being used for harm as well. That goes for fake news, foreign interference in elections, and hate speech, as well as developers and data privacy. We didn't take a broad enough view of our responsibility, and that was a big mistake. It was my mistake, and I'm sorry. I started Facebook, I run it, and I'm responsible for what happens here.

So now we have to go through every part of our relationship with people and make sure we're taking a broad enough view of our responsibility.

It's not enough to just connect people, we have to make sure those connections are positive. It's not enough to just give people a voice, we have to make sure people aren't using it to hurt people or spread misinformation. It's not enough to give people control of their information, we have to make sure developers they've given it to are protecting it too. Across the board, we have a responsibility to not just build tools, but to make sure those tools are used for good.

It will take some time to work through all of the changes we need to make, but I'm committed to getting it right.

That includes improving the way we protect people's information and safeguard elections around the world. Here are a few key things we're doing:

II. Cambridge Analytica

Over the past few weeks, we've been working to understand exactly what happened with Cambridge Analytica and taking steps to make sure this doesn't happen again. We took important actions to prevent this from happening again today four years ago, but we also made mistakes, there's more to do, and we need to step up and do it.

A. What Happened

In 2007, we launched the Facebook Platform with the vision that more apps should be social. Your calendar should be able to show your friends' birthdays, your maps should show where your friends live, and your address book should show their pictures. To do this, we enabled people to log into apps and share who their friends were and some information about them.

In 2013, a Cambridge University researcher named Aleksandr Kogan created a personality quiz app. It was installed by around 300,000 people who agreed to share some of their Facebook information as well as some information from their friends whose privacy settings allowed it. Given the way our platform worked at the time this meant Kogan was able to access some information about tens of millions of their friends.

In 2014, to prevent abusive apps, we announced that we were changing the entire platform to dramatically limit the Facebook information apps could access. Most importantly, apps like Kogan's could no longer ask for information about a person's friends unless their friends had also authorized the app. We also required developers to get approval from Facebook before they could request any data beyond a user's public profile, friend list, and e-mail address. These actions would prevent any app like Kogan's from being able to access as much Facebook data today.

In 2015, we learned from journalists at *The Guardian* that Kogan had shared data from his app with Cambridge Analytica. It is against our policies for developers to share data without people's consent, so we immediately banned Kogan's app from our platform, and demanded that Kogan and other entities he gave the data to, including Cambridge Analytica, formally certify that they had deleted all improperly acquired data—which they ultimately did.

Last month, we learned from *The Guardian, The New York Times* and Channel 4 that Cambridge Analytica may not have deleted the data as they had certified. We immediately banned them from using any of our services. Cambridge Analytica claims they have already deleted the data and has agreed to a forensic audit by a firm we hired to investigate this. We're also working with the U.K. Information Commissioner's Office, which has jurisdiction over Cambridge Analytica, as it completes its investigation into what happened.

B. What We Are Doing

We have a responsibility to make sure what happened with Kogan and Cambridge Analytica doesn't happen again. Here are some of the steps we're taking:

- *Safeguarding our platform.* We need to make sure that developers like Kogan who got access to a lot of information in the past can't get access to as much information going forward.

- We made some big changes to the Facebook platform in 2014 to dramatically restrict the amount of data that developers can access and to proactively review the apps on our platform. This makes it so a developer today can't do what Kogan did years ago.
- But there's more we can do here to limit the information developers can access and put more safeguards in place to prevent abuse.
  - We're removing developers' access to your data if you haven't used their app in three months.
  - We're reducing the data you give an app when you approve it to only your name, profile photo, and e-mail address. That's a lot less than apps can get on any other major app platform.
  - We're requiring developers to not only get approval but also to sign a contract that imposes strict requirements in order to ask anyone for access to their posts or other private data.
  - We're restricting more APIs like groups and events. You should be able to sign into apps and share your public information easily, but anything that might also share other people's information—like other posts in groups you're in or other people going to events you're going to—will be much more restricted.
  - Two weeks ago, we found out that a feature that lets you look someone up by their phone number and e-mail was abused. This feature is useful in cases where people have the same name, but it was abused to link people's public Facebook information to a phone number they already had. When we found out about the abuse, we shut this feature down.

- *Investigating other apps.* We're in the process of investigating every app that had access to a large amount of information before we locked down our platform in 2014. If we detect suspicious activity, we'll do a full forensic audit. And if we find that someone is improperly using data, we'll ban them and tell everyone affected.
- *Building better controls.* Finally, we're making it easier to understand which apps you've allowed to access your data. This week we started showing everyone a list of the apps you've used and an easy way to revoke their permissions to your data. You can already do this in your privacy settings, but we're going to put it at the top of News Feed to make sure everyone sees it. And we also told everyone whose Facebook information may have been shared with Cambridge Analytica.

Beyond the steps we had already taken in 2014, I believe these are the next steps we must take to continue to secure our platform.

III. Russian Election Interference

Facebook's mission is about giving people a voice and bringing people closer together. Those are deeply democratic values and we're proud of them. I don't want anyone to use our tools to undermine democracy. That's not what we stand for.

We were too slow to spot and respond to Russian interference, and we're working hard to get better. Our sophistication in handling these threats is growing and improving quickly. We will continue working with the government to understand the full extent of Russian interference, and we will do our part not only to ensure the integrity of free and fair elections around the world, but also to give everyone a voice and to be a force for good in democracy everywhere.

A. What Happened

Elections have always been especially sensitive times for our security team, and the 2016 U.S. presidential election was no exception.

Our security team has been aware of traditional Russian cyber threats—like hacking and malware—for years. Leading up to Election Day in November 2016, we detected and dealt with several threats with ties to Russia. This included activity by a group called APT28, that the U.S. Government has publicly linked to Russian military intelligence services.

But while our primary focus was on traditional threats, we also saw some new behavior in the summer of 2016 when APT28-related accounts, under the banner of DC Leaks, created fake personas that were used to seed stolen information to journalists. We shut these accounts down for violating our policies.

After the election, we continued to investigate and learn more about these new threats. What we found was that bad actors had used coordinated networks of fake accounts to interfere in the election: promoting or attacking specific candidates and

causes, creating distrust in political institutions, or simply spreading confusion. Some of these bad actors also used our ads tools.

We also learned about a disinformation campaign run by the Internet Research Agency (IRA)—a Russian agency that has repeatedly acted deceptively and tried to manipulate people in the U.S., Europe, and Russia. We found about 470 accounts and pages linked to the IRA, which generated around 80,000 Facebook posts over about a two-year period.

Our best estimate is that approximately 126 million people may have been served content from a Facebook Page associated with the IRA at some point during that period. On Instagram, where our data on reach is not as complete, we found about 120,000 pieces of content, and estimate that an additional 20 million people were likely served it.

Over the same period, the IRA also spent approximately $100,000 on more than 3,000 ads on Facebook and Instagram, which were seen by an estimated 11 million people in the United States. We shut down these IRA accounts in August 2017.

B. What We Are Doing

There's no question that we should have spotted Russian interference earlier, and we're working hard to make sure it doesn't happen again. Our actions include:

- *Building new technology to prevent abuse.* Since 2016, we have improved our techniques to prevent nation states from interfering in foreign elections, and we've built more advanced AI tools to remove fake accounts more generally. There have been a number of important elections since then where these new tools have been successfully deployed. For example:
  - In France, leading up to the presidential election in 2017, we found and took down 30,000 fake accounts.
  - In Germany, before the 2017 elections, we worked directly with the election commission to learn from them about the threats they saw and to share information.
  - In the U.S. Senate Alabama special election last year, we deployed new AI tools that proactively detected and removed fake accounts from Macedonia trying to spread misinformation.
  - We have disabled thousands of accounts tied to organized, financially motivated fake news spammers. These investigations have been used to improve our automated systems that find fake accounts.
  - Last week, we took down more than 270 additional pages and accounts operated by the IRA and used to target people in Russia and Russian speakers in countries like Azerbaijan, Uzbekistan and Ukraine. Some of the pages we removed belong to Russian news organizations that we determined were controlled by the IRA.
- *Significantly increasing our investment in security.* We now have about 15,000 people working on security and content review. We'll have more than 20,000 by the end of this year.
  - I've directed our teams to invest so much in security—on top of the other investments we're making—that it will significantly impact our profitability going forward. But I want to be clear about what our priority is: protecting our community is more important than maximizing our profits.
- *Strengthening our advertising policies.* We know some Members of Congress are exploring ways to increase transparency around political or issue advertising, and we're happy to keep working with Congress on that. But we aren't waiting for legislation to act.
  - From now on, every advertiser who wants to run political or issue ads will need to be authorized. To get authorized, advertisers will need to confirm their identity and location. Any advertiser who doesn't pass will be prohibited from running political or issue ads. We will also label them and advertisers will have to show you who paid for them. We're starting this in the U.S. and expanding to the rest of the world in the coming months.
  - For even greater political ads transparency, we have also built a tool that lets anyone see all of the ads a page is running. We're testing this in Canada now and we'll launch it globally this summer. We're also creating a searchable archive of past political ads.
  - We will also require people who manage large pages to be verified as well. This will make it much harder for people to run pages using fake accounts, or to grow virally and spread misinformation or divisive content that way.

- In order to require verification for all of these pages and advertisers, we will hire thousands of more people. We're committed to getting this done in time for the critical months before the 2018 elections in the U.S. as well as elections in Mexico, Brazil, India, Pakistan and elsewhere in the next year.
- These steps by themselves won't stop all people trying to game the system. But they will make it a lot harder for anyone to do what the Russians did during the 2016 election and use fake accounts and pages to run ads. Election interference is a problem that's bigger than any one platform, and that's why we support the Honest Ads Act. This will help raise the bar for all political advertising online.

- *Sharing information.* We've been working with other technology companies to share information about threats, and we're also cooperating with the U.S. and foreign governments on election integrity.

At the same time, it's also important not to lose sight of the more straightforward and larger ways Facebook plays a role in elections.

In 2016, people had billions of interactions and open discussions on Facebook that may never have happened offline. Candidates had direct channels to communicate with tens of millions of citizens. Campaigns spent tens of millions of dollars organizing and advertising online to get their messages out further. And we organized "get out the vote" efforts that helped more than 2 million people register to vote who might not have voted otherwise.

Security—including around elections—isn't a problem you ever fully solve. Organizations like the IRA are sophisticated adversaries who are constantly evolving, but we'll keep improving our techniques to stay ahead. And we'll also keep building tools to help more people make their voices heard in the democratic process.

IV. Conclusion

My top priority has always been our social mission of connecting people, building community and bringing the world closer together. Advertisers and developers will never take priority over that as long as I'm running Facebook.

I started Facebook when I was in college. We've come a long way since then. We now serve more than 2 billion people around the world, and every day, people use our services to stay connected with the people that matter to them most. I believe deeply in what we're doing. And when we address these challenges, I know we'll look back and view helping people connect and giving more people a voice as a positive force in the world.

I realize the issues we're talking about today aren't just issues for Facebook and our community—they're challenges for all of us as Americans. Thank you for having me here today, and I'm ready to take your questions.

Chairman GRASSLEY. I will remind members that maybe were not here when I had my opening comments that we are operating under the five-minute rule, and that applies to the——

[Laughter.]

Chairman GRASSLEY. The five-minute rule, and that applies to those of us who are chairing the Committee as well.

I will start with you. Facebook handles extensive amounts of personal data for billions of users. A significant amount of that data is shared with third-party developers who utilize your platform. As of early this year, you did not actively monitor whether that data was transferred by such developers to other parties. Moreover, your policies only prohibit transfers by developers to parties seeking to profit from such data.

Number one, besides Professor Kogan's transfer and now potentially Cubeyou, do you know of any instances where user data was improperly transferred to a third party in breach of Facebook's terms? If so, how many times has that happened, and was Facebook only made aware of that transfer by some third party?

Mr. ZUCKERBERG. Mr. Chairman, thank you. As I mentioned, we are now conducting a full investigation into every single app that had access to a large amount of information before we locked down

platform to prevent developers from accessing this information around 2014. We believe that we are going to be investigating many apps, tens of thousands of apps, and if we find any suspicious activity, we are going to conduct a full audit of those apps to understand how they are using their data and if they are doing anything improper. And if we find it they are doing anything improper, we will ban them from Facebook and we will tell everyone affected.

As for past activity, I do not have all the examples of apps that we have banned here, but if you would like, I can have my team follow up with you after this.

Chairman GRASSLEY. OK. Have you ever required an audit to ensure the deletion of improperly transferred data, and if so, how many times?

Mr. ZUCKERBERG. Mr. Chairman, yes, we have. I do not have the exact figure on how many times we have, but overall, the way we have enforced our platform policies in the past is we have looked at patterns of how apps have used our APIs and accessed information, as well as looked into reports that people have made to us about apps that might be doing sketchy things.

Going forward, we are going to take a more proactive position on this and do much more regular spot-checks and other reviews of apps, as well as increasing the amount of audits that we do. And again, I can make sure that our team follows up with you on anything about the specific past stats that would be interesting.

Chairman GRASSLEY. I was going to assume that sitting here today you have no idea, and if I am wrong on that, if you are able—you are telling me I think that you are able to supply those figures to us at least as of this point.

Mr. ZUCKERBERG. Mr. Chairman, I will have my team follow up with you on what information we have.

[The information referred to follows:]

Do you know of any instances where user data was improperly transferred to a third party in breach of Facebook's terms? If so, how many times has that happened, and was Facebook only made aware of that transfer by some third party?

Facebook's policies regarding third-party usage of its platform technologies have prohibited—and continue to prohibit—those third-party app developers from selling or licensing user data obtained from Facebook and from sharing any user data obtained from Facebook with any ad network, data broker, or other advertising or monetization-related service. We will investigate all apps that had access to large amounts of information before we changed our platform in 2014 to reduce data access, and we will conduct a full audit of any app with suspicious activity.

Have you ever required an audit to ensure the deletion of improperly transferred data? And if so, how many times?

We use a variety of tools to enforce Facebook policies against violating parties, including developers. We review tens of thousands of apps per year and regularly disapprove noncompliant apps as part of our proactive review process. We also use tools like cease and desist letters, account suspensions, letter agreements, and civil litigation. For example, since 2006, Facebook has sent over 1,150 cease-and-desist letters to over 1,600 targets. In 2017, we took action against about 370,000 apps, ranging from imposing certain restrictions to removal of the app from the platform. Moreover, we have required parties who have procured our data without authorization to delete that data. We have invested significant resources in these efforts. Facebook is presently investigating apps that had access to large amounts of information before we changed our platform policies in 2014 to significantly reduce the data apps could access. To date around 200 apps (from a handful of developers: Kogan, AIQ, Cube You, the Cambridge Psychometrics Center, myPersonality, and AIQ) have been suspended—pending a thorough investigation into whether they did in fact misuse any data.

Additionally, we have suspended an additional 14 apps, which were installed by around one thousand people. They were all created after 2014, after we made changes to more tightly restrict our platform APIs to prevent abuse. However, these apps appear to be linked to AIQ, which was affiliated with Cambridge Analytica. So, we have suspended them while we investigate further. Any app that refuses to take part in or fails our audit will be banned.

Chairman GRASSLEY. OK. Right now, you have no certainty of whether or not—how much of that is going on, right? OK.

Facebook collects massive amounts of data from consumers, including content, networks, contact lists, device information, location, and information from third parties, yet your data policy is only a few pages long and provides consumers with only a few examples of what is collected and how it might be used. The examples given emphasize benign uses such as connecting with friends, but your policy does not give any indication for more controversial issues of such data.

My question: Why does Facebook not disclose to its users all the ways the data might be used by Facebook and other third parties, and what is Facebook's responsibility to inform users about that information?

Mr. ZUCKERBERG. Mr. Chairman, I believe it is important to tell people exactly how the information that they share on Facebook is going to be used. That is why every single time you go to share something on Facebook, whether it is a photo in Facebook or a message in Messenger or WhatsApp, every single time, there is a control right there about who you are going to be sharing it with, whether it is your friends or public or a specific group, and you can change that and control that in line.

To your broader point about the privacy policy, this gets into an issue that I think we and others in the tech industry have found challenging, which is that long privacy policies are very confusing. And if you make it long and spell out all the detail, then you are probably going to reduce the percent of people who read it and make it accessible to them. So one of the things that we have struggled with over time is to make something that is as simple as possible so people can understand it, as well as giving them controls in line in the product in the context of when they are trying to actually use them, taking into account that we do not expect that most people will want to go through and read a full legal document.

Chairman GRASSLEY. Senator Nelson.

Senator NELSON. Thank you, Mr. Chairman.

Yesterday, when we talked, I gave the relatively harmless example that I am communicating with my friends on Facebook and indicate that I love a certain kind of chocolate, and all of a sudden, I start receiving advertisements for chocolate. What if I do not want to receive those commercial advertisements? So your Chief Operating Officer, Ms. Sandberg, suggested on the *NBC Today* show that Facebook users who do not want their personal information used for advertising might have to pay for that protection, pay for it. Are you actually considering having Facebook users pay for you not to use that information?

Mr. ZUCKERBERG. Senator, people have a control over how their information is used in ads in the product today, so if you want to

have an experience where your ads are not targeted using all the information that we have available, you can turn off third-party information. What we have found is that even though some people do not like ads, people really do not like ads that are not relevant. And while there is some discomfort for sure with using information in making ads more relevant, the overwhelming feedback that we get from our community is that people would rather have us show relevant content there than not.

So we offer this control that you are referencing. Some people use it. It is not the majority of people on Facebook. And I think that that is a good level of control to offer. I think what Sheryl was saying was that in order to not run ads at all, we would still need some sort of business model.

Senator NELSON. And that is your business model. And I use the harmless example of chocolate, but if it got into a more personal thing, communicating with friends, and I want to cut it off, I am going to have to pay you in order not to send me, using my personal information, something that I do not want. That in essence is what I understood Ms. Sandberg to say. Is that correct?

Mr. ZUCKERBERG. Yes, Senator. Although, to be clear, we do not offer an option today for people to pay to not show ads. We think offering an ad-supported service is the most aligned with our mission of trying to help connect everyone in the world because we want to offer a free service that everyone can afford.

Senator NELSON. OK.

Mr. ZUCKERBERG. That is the only way that we can reach billions of people.

Senator NELSON. So, therefore, you consider my personally identifiable data the company's data, not my data, is that it?

Mr. ZUCKERBERG. No, Senator. Actually, the first line of our terms of service say that you control and own the information and content that you put on Facebook.

Senator NELSON. Well, the recent scandal is obviously frustrating not only because it affected 87 million but because it seems to be part of a pattern of lax data practices by the company going back years. So back in 2011 it was a settlement with the FTC and now we discover yet another instance where the data failed to be protected. When you discovered the Cambridge Analytica that had fraudulently obtained all this information, why did you not inform those 87 million?

Mr. ZUCKERBERG. When we learned in 2015 that Cambridge Analytica had bought data from an app developer on Facebook that people had shared it with, we did take action. We took down the app, and we demanded that both the app developer and Cambridge Analytica delete and stop using any data that they had. They told us that they did this. In retrospect, it was clearly a mistake to believe them.

Senator NELSON. Yes.

Mr. ZUCKERBERG. We should have followed up and done a full audit then, and that is not a mistake that we will make again.

Senator NELSON. Yes, you did that, and you apologized for it, but you did not notify them. And do you think that you have an ethical obligation to notify 87 million Facebook users?

Mr. ZUCKERBERG. Senator, when we heard back from Cambridge Analytica that they had told us that they were not using the data and they had deleted it, we considered it a closed case. In retrospect, that was clearly a mistake. We should not have taken their word for it, and we have updated our policies and how we are going to operate the company to make sure that we do not make that mistake again.

Senator NELSON. Did anybody notify the FTC?

Mr. ZUCKERBERG. No, Senator, for the same reason, that we had considered it a closed case.

Chairman GRASSLEY. Senator Thune.

Chairman THUNE. And, Mr. Zuckerberg, would you do that differently today presumably, in response to Senator Nelson's question?

Mr. ZUCKERBERG. Yes.

Chairman THUNE. This may be your first appearance before Congress, but it is not the first time that Facebook has faced tough questions about its privacy policies. *Wired* magazine recently noted that you have a 14-year history of apologizing for ill-advised decisions regarding user privacy, not unlike the one that you made just now in your opening statement. After more than a decade of promises to do better, how is today's apology different, and why should we trust Facebook to make the necessary changes to ensure user privacy and give people a clearer picture of your privacy policies?

Mr. ZUCKERBERG. Thank you, Mr. Chairman. So we have made a lot of mistakes in running the company. I think it is pretty much impossible, I believe, to start a company in your dorm room and then grow it to be the scale we are at now without making some mistakes. And because our service is about helping people connect and information, those mistakes have been different in how we try not to make the same mistake multiple times, but in general, a lot of the mistakes are around how people connect to each other just because of the nature of the service.

Overall, I would say that we are going through a broader philosophical shift in how we approach our responsibility as a company. For the first 10 or 12 years of the company, I viewed our responsibility as primarily building tools, that if we could put those tools in people's hands, then that would empower people to do good things.

What I think we have learned now across a number of issues, not just data privacy but also fake news and foreign interference in elections, is that we need to take a more proactive role and a broader view of our responsibility. It is not enough to just build tools; we need to make sure that they are used for good. And that means that we need to now take a more active view in policing the ecosystem and in watching and kind of looking out and making sure that all of the members in our community are using these tools in a way that is going to be good and healthy.

So, at the end of the day, this is going to be something where people will measure us by our results on this. It is not that I expect that anything I say here today to necessarily change people's view, but I am committed to getting this right, and I believe that over the coming years, once we fully work all these solutions through, people will see real differences.

Chairman THUNE. OK. I am glad that you all have gotten that message.

As we discussed in my office yesterday, the line between legitimate political discourse and hate speech can sometimes be hard to identify, and especially when you are relying on artificial intelligence and other technologies for the initial discovery. Can you discuss the steps that Facebook currently takes when making these evaluations, the challenges that you face, and any examples of where you may draw the line between what is and what is not hate speech?

Mr. ZUCKERBERG. Yes, Mr. Chairman. I will speak to hate speech, and then I will talk about enforcing our content policies more broadly. Actually, maybe if you are OK with it, I will go in the other order.

So, from the beginning of the company in 2004, I started in my dorm room. It was me and my roommate. We did not have AI technology that could look at the content that people were sharing, so we basically had to enforce our content policies reactively. People could share what they wanted, and then if someone in the community found it to be offensive or against our policies, they would flag it for us and we would look at it reactively.

Now, increasingly, we are developing AI tools that can identify certain classes of bad activity proactively and flag it for our team at Facebook. By the end of this year, by the way, we are going to have more than 20,000 people working on security and content review working across all these things, so when content gets flagged to us, we have those people look at it, and if it violates our policies, then we take it down.

Some problems lend themselves more easily to AI solutions than others, so hate speech is one of the hardest because determining if something is hate speech is very linguistically nuanced, right? You need to understand, you know, what a slur is and whether something is hateful not just in English, but the majority of people on Facebook use it in languages that are different across the world.

Contrast that, for example, with an area like finding terrorist propaganda, which we have actually been very successful at deploying AI tools on already. Today, as we sit here, 99 percent of the ISIS and al-Qaida content that we take down on Facebook our AI systems flag before any human sees it, so that is a success in terms of rolling out AI tools that can proactively police and enforce safety across the community.

Hate speech, I am optimistic that over a 5- to 10-year period we will have AI tools that can get into some of the nuances, the linguistic nuances of different types of content to be more accurate in flagging things for our system, but today, we are just not there on that. So a lot of this is still reactive. People flag it to us. We have people look at it. We have policies to try to make it as not subjective as possible, but until we get it more automated, there is a higher error rate than I am happy with.

Chairman THUNE. Thank you, Mr. Chairman.

Chairman GRASSLEY. Senator Feinstein.

Senator FEINSTEIN. Thanks, Mr. Chairman.

Mr. Zuckerberg, what is Facebook doing to prevent foreign actors from interfering in U.S. elections?

Mr. ZUCKERBERG. Thank you, Senator. This is one of my top priorities in 2018 is to get this right. One of my greatest regrets in running the company is that we were slow in identifying the Russian information operations in 2016. We expected them to do a number of more traditional cyber attacks, which we did identify and notify the campaigns, that they were trying to hack into them, but we were slow to identifying the type of new information operations.

Senator FEINSTEIN. When did you identify new operations?

Mr. ZUCKERBERG. It was right around the time of the 2016 election itself. So since then, we—2018 is an incredibly important year for elections, not just with the U.S. midterms but around the world. There are important elections in India, in Brazil, in Mexico and Pakistan and in Hungary, that we want to make sure that we do everything we can to protect the integrity of those elections.

Now, I have more confidence that we are going to get this right because since the 2016 election, there have been several important elections around the world where we have had a better record. There is the French Presidential election, there is the German election, there was the U.S. Senate Alabama special election last year.

Senator FEINSTEIN. Explain what is better about the record.

Mr. ZUCKERBERG. So we have deployed new AI tools that do a better job of identifying fake accounts that may be trying to interfere in elections or spread misinformation. And between those three elections, we were able to proactively remove tens of thousands of accounts before they could contribute significant harm. And the nature of these attacks, though, is that, you know, there are people in Russia whose job it is to try to exploit our systems and other Internet systems and other systems as well, so this is an arms race, right? I mean, they are going to keep getting better at this, and we need to invest and keep getting better at this, too, which is why one of the things I mentioned before is we are going to have more than 20,000 people by the end of this year working on security and content review across the company.

Senator FEINSTEIN. Speak for a moment about automated bots that spread disinformation. What are you doing to punish those who exploit your platform in that regard?

Mr. ZUCKERBERG. Well, you are not allowed to have a fake account on Facebook. Your content has to be authentic. So we build technical tools to try to identify when people are creating fake accounts, especially large networks of fake accounts like the Russians have, in order to remove all of that content.

After the 2016 election, our top priority was protecting the integrity of other elections around the world, but at the same time, we had a parallel effort to trace back to Russia the IRA activity, the Internet Research Agency activity that was part of the Russian Government that did this activity in 2016. And just last week, we were able to determine that a number of Russian media organizations that were sanctioned by the Russian regulator were operated and controlled by this Internet Research Agency. So we took the step last week that was a pretty big step for us of taking down sanctioned news organizations in Russia as part of an operation to remove 270 fake accounts and pages, part of their broader network in Russia that was actually not targeting international interference

as much as—I am sorry, let me correct that. It was primarily targeting spreading misinformation in Russia itself, as well as certain Russian-speaking neighboring countries.

Senator FEINSTEIN. How many accounts of this type have you taken down?

Mr. ZUCKERBERG. In the IRA specifically, the ones that we have pegged back to the IRA, we can identify the 470 in the American elections and the 270 that we specifically went after in Russia last week. There were many others that our systems catch, which are more difficult to attribute specifically to Russian intelligence, but the number would be in the tens of thousands of fake accounts that we remove, and I am happy to have my team follow up with you on more information if that would be helpful.

Senator FEINSTEIN. Would you, please? I think this is very important.

[The information referred to follows:]

How many accounts of this type [Russian IRA/fake accounts] have you taken down?

After the 2016 election, we learned from press accounts and statements by congressional leaders that Russian actors might have tried to interfere in the election by exploiting Facebook's ad tools. This is not something we had seen before, and so we started an investigation. We found that about 470 fake accounts associated with the IRA spent approximately $100,000 on around 3,500 Facebook and Instagram ads between June 2015 and August 2017. Our analysis also showed that these accounts used these ads to promote the roughly 120 Facebook Pages they had set up, which in turn posted more than 80,000 pieces of content between January 2015 and August 2017. More recently, we took down more than 270 Pages and accounts controlled by the IRA that primarily targeted either people living in Russia or Russian speakers around the world, including from countries neighboring Russia.

We are committed to finding and removing fake accounts. We continually update our technical systems to identify, checkpoint, and remove inauthentic accounts. We block millions of attempts to register fake accounts every day. These systems examine thousands of detailed account attributes and prioritize signals that are more difficult for bad actors to disguise, such as their connections to others on our platform. We do not share detailed descriptions of how our tools work in order to avoid providing a road map to bad actors who are trying to avoid detection. When we suspect that an account is inauthentic, we typically enroll the account in a checkpoint that requires the account holder to provide additional information or verification. We view disabling an account as a severe sanction, and we want to ensure that we are highly confident that the account violates our policies before we take permanent action. When we have confirmed that an account violates our policies, we remove the account.

Senator FEINSTEIN. If you knew in 2015 that Cambridge Analytica was using the information of Professor Kogan, why did Facebook not ban Cambridge in 2015? Why did you wait in other words?

Mr. ZUCKERBERG. Senator, that is a great question. Cambridge Analytica was not using our services in 2015 as far as we can tell, so this is clearly one of the questions I asked our team as soon as I learned about this is why did we wait until we found out about the reports last month to ban them? It is because, as of the time that we learned about their activity in 2015, they were not an advertiser, they were not running pages, so we actually had nothing to ban.

Senator FEINSTEIN. Thank you.

Thank you, Mr. Chairman.

Chairman GRASSLEY. Yes, thank you, Senator Feinstein.

Now, Senator Hatch.

STATEMENT OF HON. ORRIN HATCH,
U.S. SENATOR FROM UTAH

Senator HATCH. Well, this is the most intense public scrutiny I have seen for a tech-related hearing since the Microsoft hearing that I chaired back in the late 1990s. The recent stories about Cambridge Analytica and data mining on social media raise serious concerns about consumer privacy, and naturally, I know you understand that.

At the same time, these stories touch on the very foundation of the Internet economy and the way the websites that drive our Internet economy make money. Some have professed themselves shocked, shocked that companies like Facebook and Google share user data with advertisers. Did any of these individuals ever stop to ask themselves why Facebook and Google do not charge for access? Nothing in life is free. Everything involves tradeoffs. If you want something without having to pay money for it, you are going to have to pay for it in some other way it seems to me, and that is what we are seeing here.

And these great websites that do not charge for access, they extract value in some other way, and there is nothing wrong with that, as long as they are upfront about what they are doing. In my mind the issue here is transparency. It is consumer choice. Do users understand what they are agreeing to when they access the website or agree to terms of service? Are websites upfront about how they extract value from users, or do they hide the ball? Do consumers have the information they need to make an informed choice regarding whether or not to visit a particular website? To my mind, these are questions that we should ask or be focusing on.

Now, Mr. Zuckerberg, I remember well your first visit to Capitol Hill back in 2010. You spoke to the Senate Republican High-Tech Task Force, which I chair. You said back then that Facebook would always be free. Is that still your objective?

Mr. ZUCKERBERG. Senator, yes. There will always be a version of Facebook that is free. It is our mission to try to help connect everyone around the world and to bring the world closer together. In order to do that, we believe that we need to offer a service that everyone can afford, and we are committed to doing that.

Senator HATCH. Well, if so, how do you sustain a business model in which users do not pay for your service?

Mr. ZUCKERBERG. Senator, we run ads.

Senator HATCH. I see. That is great. Whenever a controversy like this arises, there is always a danger that Congress' response will be to step in and overregulate. Now, that has been the experience that I have had in my 42 years here. In your view, what sorts of legislative changes would help to solve the problems the Cambridge Analytica story has revealed, and what sorts of legislative changes would not help to solve this issue?

Mr. ZUCKERBERG. Senator, I think that there are few categories of legislation that make sense to consider. Around privacy specifically, there are few principles that I think it would be useful to discuss and potentially codify into law. One is around having a simple and practical set of ways that you explain what you are doing with data. And we talked a little bit earlier around the complexity of laying out this long privacy policy. It is hard to say that people,

you know, fully understand something when it is only written out in a long legal document. The stuff needs to be implemented in a way where people can actually understand it, where consumers can understand it but that can also capture all the nuances of how these services work in a way that is not overly restrictive on providing the services. That is one.

The second is around giving people complete control. This is the most important principle for Facebook. Every piece of content that you share on Facebook you own, and you have complete control over who sees it and how you share it. And you can remove it at any time. That is why every day, about 100 billion times a day, people come to one of our services and either post a photo or send a message to someone because they know that they have that control and that who they say it is going to is who sees the content. And I think that that control is something that is important that I think should apply to every service. And——

Senator HATCH. Go ahead.

Mr. ZUCKERBERG.—the third point is just around enabling innovation because some of these use cases that are very sensitive like face recognition, for example—and I think that there is a balance that is extremely important to strike here where you obtain special consent for sensitive features like face recognition, but we still need to make it so that American companies can innovate in those areas or else we are going to fall behind Chinese competitors and others around the world who have different regimes for different new features like that.

Chairman GRASSLEY. Senator Cantwell.

STATEMENT OF HON. MARIA CANTWELL,
U.S. SENATOR FROM WASHINGTON

Senator CANTWELL. Thank you, Mr. Chairman.

Welcome, Mr. Zuckerberg. Do you know who Palantir is?

Mr. ZUCKERBERG. I do.

Senator CANTWELL. Some people have referred to them as a Stanford Analytica. Do you agree?

Mr. ZUCKERBERG. Senator, I have not heard that.

Senator CANTWELL. OK. Do you think Palantir taught Cambridge Analytica—press reports are saying—how to do these tactics?

Mr. ZUCKERBERG. Senator, I do not know.

Senator CANTWELL. Do you think that Palantir has ever scraped data from Facebook?

Mr. ZUCKERBERG. Senator, I am not aware of that.

Senator CANTWELL. OK. Do you think that during the 2016 campaign, as Cambridge Analytica was providing support to the Trump campaign under Project Alamo, were there any Facebook people involved in that sharing of technique and information?

Mr. ZUCKERBERG. Senator, we provided support to the Trump campaign similar to what we provide to any advertiser or campaign who asks for it.

Senator CANTWELL. So that was a yes? Is that a yes?

Mr. ZUCKERBERG. Senator, can you repeat the specific question? I just want to make sure I get——

Senator CANTWELL. Yes.

Mr. ZUCKERBERG.—specifically what you are asking.

Senator CANTWELL. During the 2016 campaign, Cambridge Analytica worked with the Trump campaign to refine tactics, and were Facebook employees involved in that?

Mr. ZUCKERBERG. Senator, I do not know that our employees were involved with Cambridge Analytica, although I know that we did help out with the Trump campaign overall in sales support in the same way that we do with other campaigns.

Senator CANTWELL. So they may have been involved and all working together during that time period? Maybe that is something your investigation will find out?

Mr. ZUCKERBERG. Senator, I can certainly have my team get back to you on any specifics there that I do not know sitting here today.

Senator CANTWELL. Have you heard of Total Information Awareness? Do you know what I am talking about?

Mr. ZUCKERBERG. No, I do not.

Senator CANTWELL. OK. Total Information Awareness was 2003, John Ashcroft and others trying to do similar things to what I think is behind all of this, geopolitical forces trying to get data and information to influence a process. So when I look at Palantir and what they are doing and I look at WhatsApp, which is another acquisition, and I look at where you are from the 2011 Consent Decree and where you are today, I am thinking is this guy outfoxing the foxes, or is he going along with what is a major trend in an information age to try to harvest information for political forces?

And so my question to you is do you see that those applications, that those companies Palantir and even WhatsApp are going to fall into the same situation that you have just fallen into over the last several years?

Mr. ZUCKERBERG. Senator, I am not sure specifically. Overall, I do think that these issues around information access are challenging. To the specifics about those apps, I am not really that familiar with what Palantir does. WhatsApp collects very little information and I think is less likely to have the kind of issues because of the way that the service is architected, but certainly, I think that these are broad issues across the tech industry.

Senator CANTWELL. Well, I guess, given the track record where Facebook is and why you are here today, I guess people would say that they did not act boldly enough. And the fact that people like John Bolton basically was an investor—in a *New York Times* article earlier—I guess it was actually last month that the Bolton PAC was obsessed with how America was becoming limp-wristed and spineless and it wanted research and messaging for national security issues.

So the fact that, you know, there are a lot of people who are interested in this larger effort, and what I think my constituents want to know is was this discussed at your Board meetings, and what are the applications and interests that are being discussed without putting real teeth into this? We do not want to come back to this situation again. I believe you have all the talent. My question is whether you have all the will to help us solve this problem?

Mr. ZUCKERBERG. Yes, Senator. So data privacy and foreign interference in elections are certainly topics that we have discussed at the Board meeting. These are some of the biggest issues that the

company has faced, and we feel a huge responsibility to get these right.

Senator CANTWELL. Do you believe the European regulations should be applied here in the U.S.?

Mr. ZUCKERBERG. Senator, I think everyone in the world deserves good privacy protection, and regardless of whether we implement the exact same regulation—I would guess that it would be somewhat different because we have somewhat different sensibilities in the U.S. as to other countries—we are committed to rolling out the controls and the affirmative consent and the special controls around sensitive types of technology like face recognition that are required in GDP are. We are doing that around the world. So I think it is certainly worth discussing whether we should have something similar in the U.S., but what I would like to say today is that we are going to go forward and implement that, regardless of what the regulatory outcome is.

Chairman GRASSLEY. Senator Wicker. Senator Thune will chair next. Senator Wicker.

STATEMENT OF HON. ROGER WICKER,
U.S. SENATOR FROM MISSISSIPPI

Senator WICKER. Thank you, Mr. Chairman.

And, Mr. Zuckerberg, thank you for being with us. My question is going to be sort of a follow-up on what Senator Hatch was talking about. And let me agree with his advice that we do not want to overregulate to the point where we are stifling innovation and investment.

I understand with regard to suggested rules or suggested legislation for internet privacy there are at least two schools of thought out there. One would be the ISPs, the internet service providers, who are advocating for privacy protections for consumers that apply to all online entities equally across the entire Internet ecosystem. Now, Facebook is an edge provider on the other hand. It is my understanding that many edge providers such as Facebook may not support that effort because edge providers have different business models than the ISPs and should not be considered like services.

So do you think we need consistent privacy protections for consumers across the entire Internet ecosystem that are based on the type of consumer information being collected, used, or shared, regardless of the entity doing the collecting, using, or sharing?

Mr. ZUCKERBERG. Senator, this is an important question. I would differentiate between ISPs, which I consider to be the pipes of the internet, and the platforms like Facebook or Google or Twitter, YouTube that are the apps or platforms on top of that. I think in general, the expectations that people have of the pipes are somewhat different from the platforms, so there might be areas where there needs to be more regulation in one and less on the other, but then I think there are going to be other places where there needs to be more regulation of the other type.

Specifically, though, on the pipes, one of the important issues that I think we face and have debated is——

Senator WICKER. When you say pipes, you mean?

Mr. ZUCKERBERG. ISPs.

Senator WICKER. The ISPs.

Mr. ZUCKERBERG. Yes. And I know net neutrality has been a hotly debated topic, and one of the reasons why I have been out there saying that I think that that should be the case is because, you know, I look at my own story of when I was getting started building Facebook at Harvard, you know, I only had one option for an ISP to use, and if I had to pay extra in order to make it so that my app could potentially be seen or used by other people, then we probably would not be here today.

Senator WICKER. OK, but we are talking about privacy concerns. And let me just say we will have to follow up on this, but I think you and I agree this is going to be one of the major items of debate if we have to go forward and address internet privacy from a governmental standpoint.

Let me move on to another couple of items. Is it true, as was recently publicized, that Facebook collects the call and text histories of its users that use android phones?

Mr. ZUCKERBERG. Senator, we have an app called Messenger for sending messages to your Facebook friends, and that app offers people an option to sync their text messages into the messaging app and to make it so that—basically, so you can have one app where it has both your texts and your Facebook messages in one place. We also allow people the option——

Senator WICKER. You can opt in or out of that?

Mr. ZUCKERBERG. Yes.

Senator WICKER. Is it easy to opt out?

Mr. ZUCKERBERG. It is opt-in. You have to affirmatively say that you want to sync that information before we get access to it.

Senator WICKER. Unless you opt in, you do not collect that call and text history?

Mr. ZUCKERBERG. That is correct.

Senator WICKER. And is this practice done at all with minors or do you make an exception there for persons aged 13 to 17?

Mr. ZUCKERBERG. I do not know. We can follow up on that.

Senator WICKER. OK. Do that. And let us know.

[The information referred to follows:]

Does Facebook allow minors (13–17) to opt in to share their call and text history?

Call and text history logging is part of an opt-in feature that lets people import contact information to help them connect with people they know on Facebook and Messenger. We introduced the call and text history component of this feature for Android users several years ago, and currently offer it in Messenger and Facebook Lite, a lightweight version of Facebook, on Android.

We've reviewed this feature to confirm that Facebook does not collect the content of messages—and will delete all logs older than one year. In the future, the client will only upload to our servers the information needed to offer this feature—not broader data such as the time of calls. We do allow people from 13 to 17 to opt into this service. However, we do take other steps to protect teens on Facebook and Messenger:

- We provide education before allowing teens to post publicly.
- We don't show search results based on specific profile data (high school, birthday/age, and hometown, or current city) of teens to unconnected adults when the adults search on Facebook.
- Unconnected adults can't message minors who are 13–17.
- We have age limits for advertisements. For example, ads for dating sites, financial services and other products or services are gated to users under 18.
- We've also helped many teenagers with information about bullying prevention campaigns and online safety tips.

Senator WICKER. And one other thing. There have been reports that Facebook can track a user's Internet browsing activity even after that user has logged off of the Facebook platform. Can you confirm whether or not this is true?

Mr. ZUCKERBERG. Senator, I want to make sure I get this accurate so it would probably be better to have my team follow up afterwards.

Senator WICKER. So you do not know?

Mr. ZUCKERBERG. I know that people use cookies on the internet and that you can probably correlate activity between sessions. We do that for a number of reasons, including security and including measuring ads to make sure that the ad experiences are the most effective, which, of course, people can opt out of. But I want to make sure that I am precise in my answer so——

Senator WICKER. Well, when you get——

Mr. ZUCKERBERG. —let me follow up with you after.

Senator WICKER.—back to me, sir, would you also let us know how Facebook discloses to its users that it is engaging in this type of tracking, if Facebook is in fact tracking users after they have logged off the platform?

Mr. ZUCKERBERG. Yes.

[The information referred to follows:]

There have been reports that Facebook can track users' Internet browsing activity even after that user has logged off of the Facebook platform. Can you confirm whether or not this is true? Would you also let us know how Facebook discloses to its users that engaging in this type of tracking gives us that result of tracking between devices?

When people visit apps or websites that feature our technologies—like the Facebook Like or Comment button—our servers automatically log (i) standard browser or app records of the fact that a particular device or user visited the website or app (this connection to Facebook's servers occurs automatically when a person visits a website or app that contains our technologies, such as a Like button, and is an inherent function of Internet design); and (ii) any additional information the publisher of the app or website chooses to share with Facebook about the person's activities on that site (such as the fact that a purchase was made on the site). This is a standard feature of the Internet, and most websites and apps share this same information with multiple different third-parties whenever people visit their website or app. For example, the Senate Commerce Committee's website shares information with Google and its affiliate DoubleClick and with the analytics company Webtrends. This means that, when a person visits the Committee's website, it sends browser information about their visit to each one of those third parties. More information about how this works is available at *https://newsroom.fb.com/news/2018/04/data-off-facebook/*.

When the person visiting a website featuring Facebook's tools is not a registered Facebook user, Facebook does not have information identifying that individual, and it does not create profiles for this individual.

We use the browser and app logs that apps and websites send to us—described above—in the following ways for non-Facebook users. First, these logs are critical to protecting the security of Facebook and to detecting or preventing fake account access. For example, if a browser has visited hundreds of sites in the last five minutes, that's a sign the device might be a bot, which would be an important signal of a potentially inauthentic account if that browser then attempted to register for an account. Second, we aggregate those logs to provide summaries and insights to websites and apps about how many people visit or use their product or use specific features like our Like button—but without providing any information about a specific person. We do not create profiles for non-Facebook users, nor do we use browser and app logs for non-Facebook users to show targeted ads from our advertisers to them or otherwise seek to personalize the content they see. However, we may take the opportunity to show a general ad that is unrelated to the attributes of the person or an ad encouraging the non-user to sign up for Facebook.

When the individual is a Facebook user, we are also able to use this information to personalize their experiences on Facebook, whether or not they are logged out,

but we will not target ads to users relying on this information unless the user allows this in their privacy settings. We do not sell or share this information with third-parties.

Senator WICKER. And thank you very much.

Chairman THUNE [presiding]. Thank you, Senator Wicker. Senator Leahy is up next.

STATEMENT OF HON. PATRICK LEAHY, U.S. SENATOR FROM VERMONT

Senator LEAHY. Thank you.

Mr. Zuckerberg, I assume Facebook has been served subpoenas from Special Counsel Mueller's office. Is that correct?

Mr. ZUCKERBERG. Yes.

Senator LEAHY. Have you or anyone at Facebook been interviewed by the Special Counsel's office?

Mr. ZUCKERBERG. Yes.

Senator LEAHY. Have you been interviewed?

Mr. ZUCKERBERG. I have not. I have not.

Senator LEAHY. Others have?

Mr. ZUCKERBERG. I believe so. And I want to be careful here because our work with the Special Counsel is confidential, and I want to make sure that in an open session I am not revealing something that is confidential.

Senator LEAHY. I understand. I just want to make clear that you have been contacted, and you have had subpoenas.

Mr. ZUCKERBERG. Actually, let me clarify that. I actually am not aware of a subpoena. I believe that there may be, but I know we are working with them.

Senator LEAHY. Thank you. Six months ago, your General Counsel promised us that you were taking steps to prevent Facebook from serving, as it is called, as an unwitting co-conspirator in Russian interference. But these unverified divisive pages are on Facebook today. They look a lot like the anonymous groups the Russian agencies used to spread propaganda during the 2016 election. Are you able to confirm whether they are Russian-created groups? Yes or no?

Mr. ZUCKERBERG. Senator, are you asking about those specifically?

Senator LEAHY. Yes.

Mr. ZUCKERBERG. Senator, last week, we actually announced a major change to our ads-and-pages policies that we will be verifying the identity of every single——

Senator LEAHY. I am asking about——

Mr. ZUCKERBERG.—advertiser——

Senator LEAHY.—specific ones. Do you know whether they are?

Mr. ZUCKERBERG. I am not familiar with those pieces of content specifically.

Senator LEAHY. But if you decided this policy a week ago, you would be able to verify them?

Mr. ZUCKERBERG. We are working on that now. What we are doing is we are going to verify the identity of any advertiser who is running a political- or issue-related ad. This is basically what the Honest Ads Act is proposing, and we are following that, and we are also going to do that for pages so——

Senator LEAHY. But you cannot answer on these?

Mr. ZUCKERBERG. I am not familiar with those specific cases.

Senator LEAHY. Will you find out the answer and get back to me?

Mr. ZUCKERBERG. I will have my team get back to you.

[The information referred to follows:]

Six months ago, your general counsel promised us you were taking steps to prevent Facebook from serving what I call unwitting conspiracy Russian interference. But these unverified, divisive pages are on Facebook today. They look a lot like Russian agents used to spread propaganda during the 2016 election. Are you able to confirm whether they are Russian groups, yes or no?

In general, we take aggressive investigative steps to identify and disable groups that conduct coordinated inauthentic activities on the platform, but it is extremely challenging to definitively attribute online activity to particular threat actors. We often rely on information from others, like information from the government, to identify actors behind abuse that we observe and to better understand these issues. We would need more information in order to review the specific Pages referenced at the hearing.

Mr. ZUCKERBERG. I do think it is worth adding, though, that we are going to do the same verification of the identity and location of admins who are running large pages, so that way even if they are not going to be buying ads on our system, that will make it significantly harder for Russian interference efforts or other inauthentic efforts——

Senator LEAHY. Well, some——

Mr. ZUCKERBERG.—to try to spread information through the network.

Senator LEAHY. And it has been going on for some time, so you might say that it is about time. You know, six months ago, I asked your general counsel about Facebook's role as a breeding ground for hate speech against Rohingya refugees. Recently, U.N. investigators blamed Facebook for playing a role in inciting the possible genocide in Myanmar, and there has been genocide there. Now, you say you used AI to find this. This is the type of content I am referring to. It calls for the death of a Muslim journalist. Now, that threat went straight through your detection system, it spread very quickly, and then, it took attempt after attempt after attempt and the involvement of civil society groups to get you to remove it. Why could it not be removed within 24 hours?

Mr. ZUCKERBERG. Senator, what is happening in Myanmar is a terrible tragedy, and we need to do more.

Senator LEAHY. We all agree with that.

Mr. ZUCKERBERG. OK.

Senator LEAHY. But U.N. investigators have blamed you, blamed Facebook for playing a role in the genocide. We all agree it is terrible. How can you dedicate and will you dedicate resources to make sure such hate speech is taken down within 24 hours?

Mr. ZUCKERBERG. Yes, we are working on this. And there are three specific things that we are doing. One is we are hiring dozens of more Burmese language content reviewers because hate speech is very language-specific. It is hard to do it without people who speak the local language, and we need to ramp up our effort there dramatically.

Second is we are working with civil society in Myanmar to identify specific hate figures so we can take down their accounts rather than specific pieces of content.

And third is we are standing up a product team to do specific product changes in Myanmar and other countries that may have similar issues in the future to prevent this from happening.

Senator LEAHY. Senator Cruz and I sent a letter to Apple asking what they are going to do about Chinese censorship. My question, I will place it for the record.

Chairman THUNE. That would be great. Thank you, Senator Leahy.

Senator LEAHY. At least for the record I want to know what you will do about Chinese censorship when they come to you.

[The information referred to follows:]

I want to know what you'll do about Chinese censorship when they come to you.

Because Facebook has been blocked in China since 2009, we are not in a position to know exactly how the government would seek to apply its laws and regulations on content were we permitted to offer our service to Chinese users. Since 2013, Facebook has been a member of the Global Network Initiative (GNI), a multi-stakeholder digital rights initiative. As part of our membership, Facebook has committed to the freedom of expression and privacy standards set out in the GNI Principles—which are in turn based on the Universal Declaration of Human Rights and the United Nations Guiding Principles on Business and Human Rights—and we are independently assessed on our compliance with these standards on a biennial basis.

When something on Facebook or Instagram is reported to us as violating local law, but doesn't go against our Community Standards, we may restrict the content's availability only in the country where it is alleged to be illegal after careful legal review. We receive reports from governments and courts, as well from non-government entities such as members of the Facebook community and NGOs.

More information is available here: *https://transparency.facebook.com/content-restrictions.*

Chairman THUNE. Senator Graham is up next.

STATEMENT OF HON. LINDSEY GRAHAM,
U.S. SENATOR FROM SOUTH CAROLINA

Senator GRAHAM. Thank you.

Are you familiar with Andrew Bosworth?

Mr. ZUCKERBERG. Yes, Senator, I am.

Senator GRAHAM. He said, "So we connect more people, maybe someone dies in a terrorist attack coordinated on our tools. The ugly truth is that we believe in connecting people so deeply that anything that allows us to connect more people more often is de facto good." Do you agree with that?

Mr. ZUCKERBERG. No, Senator, I do not, and as context, Bos wrote that—Bos is what we call him internally—he wrote that as an internal note. We had a lot of discussion internally. I disagreed with it at the time that he wrote it. If you looked at the comments on the internal discussion, the vast majority——

Senator GRAHAM. Would you say——

Mr. ZUCKERBERG.—of people internally did, too.

Senator GRAHAM.—that you did a poor job as a CEO communicating your displeasure with such thoughts because if he had understood where you were, he never would have said it to begin with?

Mr. ZUCKERBERG. Well, Senator, we try to run our company in a way where people can express different opinions internally.

Senator GRAHAM. Well, this is an opinion that really disturbs me. And if somebody worked for me that said this, I would fire them.

Who is your biggest competitor?

Mr. ZUCKERBERG. Senator, we have a lot of competitors.

Senator GRAHAM. Who is your biggest?

Mr. ZUCKERBERG. I think the categories of—did you want just one? I am not sure I can give one, but can I give a bunch?

Senator GRAHAM. Yes.

Mr. ZUCKERBERG. So there are three categories I would focus on. One are the other tech platforms so Google, Apple, Amazon, Microsoft. We overlap with them in different ways.

Senator GRAHAM. Do they provide the same service you provide?

Mr. ZUCKERBERG. In different ways, different parts of it, yes.

Senator GRAHAM. Let me put it this way. If I buy a Ford and it does not work well and I do not like it, I can buy a Chevy. If I am upset with Facebook, what is the equivalent product that I can go sign up for?

Mr. ZUCKERBERG. Well, the second category that I was going to talk about are specific——

Senator GRAHAM. I am not talking about categories. I am talking about is there real competition you face? Because car companies face a lot of competition. If they make a defective car, it gets out in the world, people stop buying that car or they buy another one. Is there an alternative to Facebook in the private sector?

Mr. ZUCKERBERG. Yes, Senator. The average American uses eight different apps——

Senator GRAHAM. OK.

Mr. ZUCKERBERG.—to communicate with their friends and stay in touch with people——

Senator GRAHAM. OK.

Mr. ZUCKERBERG.—ranging from texting apps——

Senator GRAHAM. Which is the——

Mr. ZUCKERBERG.—to e-mail to——

Senator GRAHAM.—same service you provide? Is——

Mr. ZUCKERBERG. Well, we provide a number of different services.

Senator GRAHAM. Is Twitter the same as what you do?

Mr. ZUCKERBERG. It overlaps with a portion of what we do.

Senator GRAHAM. You do not think you have a monopoly?

Mr. ZUCKERBERG. It certainly does not feel like that to me.

[Laughter.]

Senator GRAHAM. OK. So it does not. So Instagram, you bought Instagram. Why did you buy Instagram?

Mr. ZUCKERBERG. Because they were very talented app developers who were making good use of our platform and understood our values.

Senator GRAHAM. It was a good business decision. My point is that one way to regulate a company is through competition, through government regulation. Here is the question that all of us got an answer. What we tell our constituents, given what has happened here, why we should let you self-regulate? What would you tell people in South Carolina that, given all the things we have just discovered here, it is a good idea for us to rely upon you to regulate your own business practices?

Mr. ZUCKERBERG. Well, Senator, my position is not that there should be no regulation.

Senator GRAHAM. OK.

Mr. ZUCKERBERG. I think the Internet has increased the importance——

Senator GRAHAM. Do you embrace regulation?

Mr. ZUCKERBERG. I think the real question, as the internet becomes more important in people's lives, is what is the right regulation, not whether there should be regulation.

Senator GRAHAM. But you as a company welcome regulation?

Mr. ZUCKERBERG. I think if it is the right regulation, then yes.

Senator GRAHAM. Do you think the Europeans have it right?

Mr. ZUCKERBERG. I think that they get things right.

Senator GRAHAM. Have you ever submitted——

[Laughter.]

Senator GRAHAM. That is true. So would you work with us in terms of what regulations you think are necessary in your industry?

Mr. ZUCKERBERG. Absolutely.

Senator GRAHAM. OK. Would you submit to us some proposed regulations?

Mr. ZUCKERBERG. Yes, and I will have my team follow up with you, so that way we can have this discussion across the different categories where I think that this discussion needs to happen.

Senator GRAHAM. I look forward to it.

[The information referred to follows:]

Would you submit to us some proposed regulations?

Facebook is generally not opposed to regulation but wants to ensure it is the right regulation. The issues facing the industry are complex, multi-faceted, and affect an important part of peoples' lives. As such, Facebook is absolutely committed to working with regulators, like Congress, to craft the right regulations. Facebook would be happy to review any proposed legislation and provide comments.

Senator GRAHAM. When you sign up for Facebook, you sign up for terms of service. Are you familiar with that?

Mr. ZUCKERBERG. Yes.

Senator GRAHAM. OK. It says, "The terms govern your use of Facebook and the products, features, apps, services, technologies, software we offer (the Facebook products or products), except where we expressly state that separate terms (and not these) apply." I am a lawyer and I have no idea what that means. But when you look at terms of service, this is what you get. Do you think the average consumer understands what they are signing up for?

Mr. ZUCKERBERG. I do not think that the average person likely reads that whole document.

Senator GRAHAM. Yes.

Mr. ZUCKERBERG. But I think that there are different ways that we can communicate that and have a responsibility to do so.

Senator GRAHAM. Do you agree with me that you better come up with different ways because this is not working?

Mr. ZUCKERBERG. Well, Senator, I think in certain areas that is true, and I think in other areas like the core part of what we do—right, if you think about just at the most basic level, people come to Facebook, Instagram, WhatsApp, Messenger about 100 billion times a day to share a piece of content or a message with a specific set of people. And I think that that basic functionality people understand because we have the controls in line every time. And given the volume of the activity and the value that people tell us

that they are getting from that, I think that that control in line does seem to be working fairly well.

Now, we can always do better, and there are other services that are complex and there is more to it than just, you know, you go and you push the photo, so I agree that in many places we could do better. But I think for the core of the service, it actually is quite clear.

Chairman THUNE. Thank you, Senator Graham.

Senator Klobuchar.

STATEMENT OF HON. AMY KLOBUCHAR,
U.S. SENATOR FROM MINNESOTA

Senator KLOBUCHAR. Thank you, Mr. Chairman.

Mr. Zuckerberg, I think we all agree that what happened here was bad. You acknowledged it was a breach of trust. And the way I explained it to my constituents is that if someone breaks into my apartment with a crowbar and they take my stuff, it is just like if the manager gave them the keys or if they did not have any locks on the doors. It is still a breach. It is still a break-in. And I believe we need to have laws and rules that are as sophisticated as the brilliant products that you have developed here, and we just have not done that yet.

And one of the areas that I have focused on is the election, and I appreciate the support that you and Facebook and now Twitter actually have given to the Honest Ads Act, a bill that you mentioned that I am leading with Senator McCain and Senator Warner. And I just want to be clear, as we work to pass this law so that we have the same rules in place to disclose political ads and issue ads as we do for TV and radio, as well as disclaimers, that you are going to take early action—as soon as June I heard—before this election so that people can view these ads, including issue ads, is that correct?

Mr. ZUCKERBERG. That is correct, Senator, and I just want to take a moment before I go into this in more detail to thank you for your leadership on this. This I think is an important area for the whole industry to move on.

The two specific things that we are doing are, one is around transparency, so now, you are going to be able to go and click on any advertiser or any page on Facebook and see all of the ads that they are running, so that actually brings advertising online on Facebook to an even higher standard than what you would have on TV or print media because there is nowhere where you can see all of the TV ads that someone is running, for example, where as you will be able to see now on Facebook whether this campaign or third party is saying different messages to different types of people. And I think that is a really important element of transparency. And the other really important piece is around verifying every single advertiser who is going to be running political or issue ads.

Senator KLOBUCHAR. I appreciate that. And Senator Warner and I have also called on Google and the other platforms to do the same, so memo to the rest of you, we have to get this done or we are going to have a patchwork of ads. And I hope that you will be working with us to pass this bill. Is that right?

Mr. ZUCKERBERG. We will.

Senator KLOBUCHAR. OK. Thank you.

Now, on the subject of Cambridge Analytica, were these people, the 87 million people, users, concentrated in certain states? Are you able to figure out where they are from?

Mr. ZUCKERBERG. I do not have that information with me——

Senator KLOBUCHAR. But you could get it?

Mr. ZUCKERBERG.—but we can follow up with your office.

Senator KLOBUCHAR. OK. Because, as we know, the election was close, and it was only thousands of votes in certain states.

You have also estimated that roughly 126 million people may have been shown content from a Facebook page associated with the Internet Research Agency. Have you determined whether any of those people were the same Facebook users whose data was shared with Cambridge Analytica? Are you able to make that determination?

Mr. ZUCKERBERG. Senator, we are investigating that now. We believe that it is entirely possible that there will be a connection there.

Senator KLOBUCHAR. OK. That seems like a big deal as we look back at that last election.

Former Cambridge Analytica employee Christopher Wiley has said that the data that it improperly obtained, that Cambridge Analytica improperly obtained from Facebook users could be stored in Russia. Do you agree that that is a possibility?

Mr. ZUCKERBERG. Sorry, are you asking if Cambridge Analytica's data could be stored in Russia?

Senator KLOBUCHAR. That is what he said this weekend on a Sunday show.

Mr. ZUCKERBERG. Senator, I do not have any specific knowledge that would suggest that, but one of the steps that we need to take now is go do a full audit of all of Cambridge Analytica's systems, understand what they are doing, whether they still have any data, to make sure that they remove all the data. If they do not, we are going to take legal action against them to do so.

That audit we have temporarily ceded that in order to let the U.K. Government complete their government investigation first because of course a government investigation takes precedence over a company doing that. But we are committed to completing this full audit and getting to the bottom of what is going on here so that way we can have more answers to this.

Senator KLOBUCHAR. OK. You earlier stated publicly and here that you would support some privacy rules so that everyone is playing by the same rules here. And you also said here that you should have notified customers earlier. Would you support a rule that would require you to notify your users of a breach within 72 hours?

Mr. ZUCKERBERG. Senator, that makes sense to me, and I think we should have our team follow up with yours to discuss the details around that more.

[The information referred to follows:]

Can you provide a breakdown of users affected by Cambridge Analytica by state?

See the state breakdown here: *https://fbnewsroomus.files.wordpress.com/2018/05/state-by-state-breakdown.pdf*.

Do you support a rule that would require you to notify your users of a breach within 72 hours?

Facebook is generally open to the idea of breach notification requirements, particularly legislation that would centralize reporting and ensure a consistent approach across the United States. For example, in Europe, the GDPR requires notification to a lead supervisory authority, rather than individual member states, in cases of a data breach. In the United States, however, there is no centralized notification scheme, and instead, reporting obligations vary widely across all 50 states. This complexity makes it harder to respond appropriately and swiftly to protect people in the event of a data breach. We believe this is an important issue and an area that is ripe for thoughtful regulation.

Senator KLOBUCHAR. Thank you. I just think part of this was when people do not even know that their data has been breached, that is a huge problem, and I also think we get to solutions faster when we get that information out there.

Thank you, and we look forward to passing this bill. We would love to pass it before the election on the Honest Ads and looking forward to better disclosure this election. Thank you.

Chairman THUNE. Thank you, Senator Klobuchar.

Senator Blunt is up next.

STATEMENT OF HON. ROY BLUNT,
U.S. SENATOR FROM MISSOURI

Senator BLUNT. Thank you, Mr. Chairman.

Mr. Zuckerberg, nice to see you. I saw you not too long after I entered the Senate in 2011. I told you when I sent my business cards down to be printed, they came back from the Senate printshop with the message that they were the first business card they had ever printed a Facebook address on. There are days when I have regretted that but more days when we get lots of information that we need to get. There are days when I wonder if the term "Facebook friends" is a little misstated. It does not seem like I have those every single day. But, you know, the platform you have created is really important.

Now, my son Charlie, who is 13, is dedicated to Instagram, so he would want to be sure I mentioned him while I was here with you.

[Laughter.]

Senator BLUNT. I have not printed that on my card yet, I will say that, but I think we have that account as well. A lot of ways to connect people. And the information obviously is an important commodity, and it is what makes your business work. I get that. However, I wonder about some of the collection efforts, and maybe we can go through largely just even yes or no and then we will get back to more expansive discussion of this.

But do you collect user data through cross-device tracking?

Mr. ZUCKERBERG. Senator, I believe we do link people's accounts between devices in order to make sure that their Facebook and Instagram and their other experiences can be synced between their devices.

Senator BLUNT. And that would also include off-line data, data that is tracking that is not necessarily linked to Facebook but linked to some device they went through Facebook on, is that right?

Mr. ZUCKERBERG. Senator, I want to make sure we get this right, so I want to have my team follow up with you on that afterwards.

Senator BLUNT. Well, now, that does not seem that complicated to me. Now, you understand this better than I do, but maybe you

can explain to me why that is complicated. Do you track devices that an individual who uses Facebook has that is connected to the device that they use for their Facebook connection but not necessarily connected to Facebook?

Mr. ZUCKERBERG. I am not sure the answer to that question.

Senator BLUNT. Really?

Mr. ZUCKERBERG. Yes. There may be some data that is necessary to provide the service that we do, but I do not have that sitting here today, so that is something I would want to follow up with you on.

[The information referred to follows:]

Do you track non-Facebook data from devices on which they have used Facebook, even if they are logged off of Facebook or the device is offline? So you don't have bundled permissions for how I can agree to what devices I may use that you may have contact with? Do you bundle that permission, or am I able to individually say what I'm willing for you to watch and what I don't want you to watch?

When people visit apps or websites that feature our technologies—like the Facebook Like or Comment button—our servers automatically log (i) standard browser or app records of the fact that a particular device or user visited the website or app (this connection to Facebook's servers occurs automatically when a person visits a website or app that contains our technologies, such as a Like button, and is an inherent function of Internet design); and (ii) any additional information the publisher of the app or website chooses to share with Facebook about the person's activities on that site (such as the fact that a purchase was made on the site). This is a standard feature of the Internet, and most websites and apps share this same information with multiple different third-parties whenever people visit their website or app. For example, the Senate Commerce Committee's website shares information with Google and its affiliate DoubleClick and with the analytics company Webtrends. This means that, when a person visits the Committee's website, it sends browser information about their visit to each one of those third parties. More information about how this works is available at *https://newsroom.fb.com/news/2018/04/data-off-facebook/*.

When the person visiting a website featuring Facebook's tools is not a registered Facebook user, Facebook does not have information identifying that individual, and it does not create profiles for this individual.

We use the browser and app logs that apps and websites send to us—described above—in the following ways for non-Facebook users. First, these logs are critical to protecting the security of Facebook and to detecting or preventing fake account access. For example, if a browser has visited hundreds of sites in the last five minutes, that's a sign the device might be a bot, which would be an important signal of a potentially inauthentic account if that browser then attempted to register for an account. Second, we aggregate those logs to provide summaries and insights to websites and apps about how many people visit or use their product or use specific features like our Like button—but without providing any information about a specific person. We do not create profiles for non-Facebook users, nor do we use browser and app logs for non-Facebook users to show targeted ads from our advertisers to them or otherwise seek to personalize the content they see. However, we may take the opportunity to show a general ad that is unrelated to the attributes of the person or an ad encouraging the non-user to sign up for Facebook.

When the individual is a Facebook user, we are also able to use this information to personalize their experiences on Facebook, whether or not they are logged out, but we will not target ads to users relying on this information unless the user allows this in their privacy settings. We do not sell or share this information with third-parties.

Senator BLUNT. Now, the FTC last year flagged cross-device tracking as one of their concerns generally that people are tracking devices that the users of something like Facebook do not know they are being tracked. How do you disclose your collection methods? Is that all in this document that I would see and agree to before I entered into a Facebook partnership?

Mr. ZUCKERBERG. Yes, Senator. So there are two ways that we do this. One is we try to be exhaustive in the legal documents

around the terms of service and privacy policies. But more importantly, we try to provide in-line controls that are in plain English that people can understand. They can either go to settings or we can show them at the top of the app periodically so that people understand all the controls and settings they have and can configure their experience the way that they want.

Senator BLUNT. So do people now give you permission to track specific devices in their contract? And if they do, is that a relatively new addition to what you do?

Mr. ZUCKERBERG. Senator, I am sorry I do not have the——

Senator BLUNT. Am I able to opt out? Am I able to say it is OK for you to track what I am saying on Facebook, but I do not want you to track what I am texting to somebody else off Facebook on an android phone?

Mr. ZUCKERBERG. Oh, OK. Yes, Senator. In general, Facebook is not collecting data from other apps that you use. There may be some specific things about the device that you are using that Facebook needs to understand in order to offer the service, but if you are using Google or you are using some texting app, unless you specifically opt in that you want to share the texting app information, Facebook would not see that.

Senator BLUNT. Has it always been that way or is that a recent addition to how you deal with those other ways that I might communicate?

Mr. ZUCKERBERG. Senator, my understanding is that that is how the mobile operating systems are architected.

Senator BLUNT. So you do not have bundled permissions for how I can agree to what devices I may use that you may have contact with? Do you bundle that permission or am I able to individually say what I am willing for you to watch and what I do not want you to watch? I think we may have to take that for the record based on everybody else's time.

[The information referred to follows:]

Do you track devices that an individual who uses Facebook has that is connected to the device that they use for their Facebook connection but not necessarily connected to Facebook?

Yes, Facebook's Data Policy specifically discloses that we associate information across different devices that people use to provide a consistent experience wherever they use Facebook.

Facebook's services inherently operate on a cross-device basis: understanding when people use our services across multiple devices helps us provide the same personalized experience wherever people use Facebook—for example, to ensure that a person's News Feed or profile contains the same content whether they access our services on their mobile phone or in a desktop computer's web browser.

In support of those and other purposes, we collect information from and about the computers, phones, connected TVs and other web-connected devices our users use that integrate with our Products, and we combine this information across a user's different devices. For example, we use information collected about a person's use of our Products on their phone to better personalize the content (including ads) or features they see when they use our Products on another device, such as their laptop or tablet, or to measure whether they took an action in response to an ad we showed them on their phone or on a different device.

Information we obtain from these devices includes:

- *Device attributes:* information such as the operating system, hardware and software versions, battery level, signal strength, available storage space, browser type, app and file names and types, and plugins.

- *Device operations:* information about operations and behaviors performed on the device, such as whether a window is foregrounded or backgrounded, or mouse movements (which can help distinguish humans from bots).
- *Identifiers:* unique identifiers, device IDs, and other identifiers, such as from games, apps or accounts people use, and Family Device IDs (or other identifiers unique to Facebook Company Products associated with the same device or account).
- *Device signals:* Bluetooth signals, and information about nearby Wi-Fi access points, beacons, and cell towers.
- *Data from device settings:* information a user allows us to receive through device settings they turn on, such as access to their GPS location, camera or photos.
- *Network and connections:* information such as the name of a user's mobile operator or ISP, language, time zone, mobile phone number, IP address, connection speed and, in some cases, information about other devices that are nearby or on their network, so we can do things like help them stream a video from their phone to their TV.
- *Cookie data:* data from cookies stored on a user's device, including cookie IDs and settings. More information is available at *https://www.facebook.com/policies/cookies/* and *https://help.instagram.com/1896641480634370?ref=ig.*

Advertisers, app developers, and publishers can send us information through Facebook Business Tools they use, including our social plug-ins (such as the Like button), Facebook Login, our APIs and SDKs, or the Facebook pixel. These partners provide information about a person's activities off Facebook—including information about their device, websites they visit, purchases they make, the ads they see, and how they use their services—whether or not they have a Facebook account or are logged into Facebook. For example, a game developer could use our API to tell us what games a person plays, or a business could tell us about a purchase a person made in its store. We also receive information about a person's online and offline actions and purchases from third-party data providers who have the rights to provide us with that person's information.

We use the information we have to deliver our Products, including to personalize features and content (including a person's News Feed, Instagram Feed, Instagram Stories and ads) and make suggestions for a user (such as groups or events they may be interested in or topics they may want to follow) on and off our Products. To create personalized Products that are unique and relevant to them, we use their connections, preferences, interests and activities based on the data we collect and learn from them and others (including any data with special protections they choose to provide); how they use and interact with our Products; and the people, places, or things they're connected to and interested in on and off our Products.

For example, if people have shared their device locations with Facebook or checked into a specific restaurant, we can show them ads from an advertiser that wants to promote its services in their area or from the restaurant. We use location-related information—such as a person's current location, where they live, the places they like to go, and the businesses and people they're near—to provide, personalize and improve our Products, including ads, for them and others. Location-related information can be based on things like precise device location (if a user has allowed us to collect it), IP addresses, and information from their and others' use of Facebook Products (such as check-ins or events they attend). We store data until it is no longer necessary to provide our services and Facebook Products, or until a person's account is deleted—whichever comes first. This is a case-by-case determination that depends on things like the nature of the data, why it is collected and processed, and relevant legal or operational retention needs. We provide advertisers with reports about the kinds of people seeing their ads and how their ads are performing, but we don't share information that personally identifies someone (information such as a person's name or e-mail address that by itself can be used to contact them or identifies who they are) unless they give us permission. For example, we provide general demographic and interest information to advertisers (for example, that an ad was seen by a woman between the ages of 25 and 34 who lives in Madrid and likes software engineering) to help them better understand their audience. We also confirm which Facebook ads led users to make a purchase or take an action with an advertiser.

Chairman THUNE. Thank you, Senator Blunt.
Next up, Senator Durbin.

STATEMENT OF HON. RICHARD DURBIN,
U.S. SENATOR FROM ILLINOIS

Senator DURBIN. Thank you very much, Mr. Chairman.

Mr. Zuckerberg, would you be comfortable sharing with us the name of the hotel you stayed in last night?

Mr. ZUCKERBERG. No.

[Laughter.]

Senator DURBIN. If you messaged anybody this week, would you share with us the names of the people you have messaged?

Mr. ZUCKERBERG. Senator, no. I would probably not choose to do that publicly here.

Senator DURBIN. I think that may be what this is all about, your right to privacy, the limits of your right to privacy, and how much you give away in modern America in the name of, quote, "connecting people around the world," a question basically of what information Facebook is collecting, who they are sending it to, and whether they ever asked me in advance my permission to do that. Is that a fair thing for a user of Facebook to expect?

Mr. ZUCKERBERG. Yes, Senator. I think everyone should have control over how their information is used. And as we have talked about in some of the other questions, I think that that is laid out in some of the documents, but more importantly, you want to give people control in the product itself. So the most import way that this happens across our services is that every day people come to our services to choose to share photos or send messages, and every single time they choose to share something, they have a control right there about who they want to share it with. But that——

Senator DURBIN. They certainly——

Mr. ZUCKERBERG.—level of control is extremely important.

Senator DURBIN. They certainly know within the Facebook pages who their friends are, but they may not know, as has happened—and you have conceded this point in the past—that sometimes that information is going way beyond their friends, and sometimes, people have made money off of sharing that information, correct?

Mr. ZUCKERBERG. Senator, you are referring I think to our developer platform, and it may be useful for me to give some background on how we set that up if that is useful.

Senator DURBIN. I have 3 minutes left, so maybe you can do that for the record because I have a couple other questions that I would like to ask.

[The information referred to follows:]

They certainly know within the Facebook pages who their friends are, but they may not know, as has happened, and you've conceded this point in the past, that sometimes that information is going way beyond their friends and sometimes people have made money off of sharing that information, correct?

Our Download Your Information or "DYI" tool is Facebook's data portability tool and was launched many years ago to let people access and download many types of information that we maintain about them. The data in DYI and in our Ads Preferences tool contain each of the interest categories that are used to show people ads, along with information about the advertisers are currently running ads based on their use of an advertiser's website or app. People also can choose not to see ads from those advertisers. We recently announced expansions to Download Your Information, which, among other things, will make it easier for people to see their data, delete it, and easily download and export it. More information is available at *https://newsroom.fb.com/news/2018/04/new-privacy-protections*.

Responding to feedback that we should do more to provide information about websites and apps that send us information when people use them, we also an-

nounced plans to build Clear History. This new feature will enable users to see the websites and apps that send us information when they use them, delete this information from their account, and turn off Facebook's ability to store it associated with their account going forward.

We have also introduced Access Your Information. This feature provides a new way for people to access and manage their information. Users can go here to delete anything from their timeline or profile that they no longer want on Facebook. They can also see their ad interests, as well as information about ads they've clicked on and advertisers who have provided us with information about them that influence the ads they see. From here, they can go to their ad settings to manage how this data is used to show them ads.

Facebook allows people to view, manage, and remove the apps that they have logged into with Facebook through the App Dashboard. We recently prompted everyone to review their App Dashboard as a part of a Privacy Checkup, and we also provided an educational notice on Facebook to encourage people to review their settings. More information about how users can manage their app settings is available at *https://www.facebook.com/help/218345114850283?helpref=about_content*.

The categories of information that an app can access are clearly disclosed before the user consents to use an app on the Facebook Platform. Users can view and edit the categories of information that apps they have used have access to through the App Dashboard.

Senator DURBIN. You have recently announced something that is called Messenger Kids. Facebook created an app allowing kids between the ages of 6 and 12 to send video and text messages through Facebook as an extension of their parent's account. They have cartoon-like stickers and other features designed to appeal to little kids, first-graders, kindergartners. On January 30, Campaign for a Commercial-Free Childhood and lots of other child development organizations warned Facebook. They pointed to a wealth of research demonstrating that excessive use of digital devices and social media is harmful to kids. It argued that young children simply are not ready to handle social media accounts at age six.

In addition, there are concerns about data that is being gathered about these kids. Now, there are certain limits in the law, we know. There is Children's Online Privacy Protection Act. What guarantees can you give us that no data from Messenger Kids is or will be collected or shared with those that might violate that law?

Mr. ZUCKERBERG. All right. Senator, so a number of things I think are important here. The background on Messenger Kids is we heard feedback from thousands of parents that they want to be able to stay in touch with their kids and call them, use apps like FaceTime when they are working late or not around and want to communicate with their kids, but they want to have complete control over that. So I think we can all agree that when your kid is six or seven, even if they have access to a phone, you want to be able to control everyone who they can contact. And there was not an app out there that did that, so we built this service to do that.

The app collects a minimum amount of information that is necessary to operate the service, so, for example, the messages that people send is something that we collect in order to operate the service. But in general, that data is not going to be shared with third parties. It is not connected to the broader Facebook experience——

Senator DURBIN. Excuse me. As a lawyer, I picked up on that word "in general," that phrase "in general." It seems to suggest that in some circumstances it will be shared with third parties.

Mr. ZUCKERBERG. No, it will not.

Senator DURBIN. All right. Would you be open to the idea that someone having reached adult age having grown up with Messenger Kids should be allowed to delete the data you have collected?

Mr. ZUCKERBERG. Senator, yes. As a matter of fact, when you become 13, which is our legal limit—we do not allow people under the age of 13 to use Facebook—you do not automatically go from having a Messenger Kids account to a Facebook account. You have to start over and get a Facebook account. So I think it is a good idea to consider making sure that all that information is deleted, and in general, people are going to be starting over when they get their Facebook or other accounts.

Senator DURBIN. I will close because I just have a few seconds. Illinois has a Biometric Information Privacy Act, our state does, which is to regulate the commercial use of facial, voice, finger, and iris scans and the like. We are now in a fulsome debate on that, and I am afraid Facebook has come down with the position of trying to carve out exceptions to that. I hope you will fill me in on how that is consistent with protecting privacy. Thank you.

[The information referred to follows:]

Illinois has a biometric information privacy act, our state does, which is to regulate the commercial use of facial, voice, finger and iris scans and the like. We're now in a fulsome debate on that and Facebook has come down on a position trying to carve out exceptions and I hope you'll fill me in on how that is consistent with protecting privacy.

We are aware of several pending measures to amend the Illinois Biometric Information Privacy Act to foster the use of technology to enhance privacy and data security and combat threats like fraud, identity theft, and impersonation. Facebook has not supported these measures or requested any organization or chamber of commerce to do so.

In 2016, Senator Terry Link, the author of the Illinois Biometric Information Privacy Act, introduced a measure (HB 6074) clarifying that the original law (1) does not apply to information derived from physical or digital photographs and (2) uses the term "scan" to mean information that is obtained from an in-person process. These clarifying amendments were consistent with industry's longstanding interpretation of the law and Facebook publicly supported them.

Facebook's advocacy is consistent with our commitment to protecting privacy. As the findings of the Illinois General Assembly confirm, when people raise privacy concerns about facial recognition, they are generally about specific uses of facial recognition. In enacting the Illinois Biometric Information Privacy Act, the General Assembly explained that its concern was "new applications of biometric-facilitated financial transactions, including finger-scan technologies at grocery stores, gas stations, and school cafeterias." 740 ILCS 14/5.

Facebook's use of facial recognition in our products, on the other hand, is very different. Facebook uses facial-recognition technology with users to provide Facebook users—who choose to join Facebook for the purpose of connecting with and sharing information about themselves with others, and affirmatively agree to Facebook's Terms of Service and Data Policy—with products and features that protect their identities and enhance their online experiences while giving them control over the technology. For example, Facebook uses facial-recognition technology to protect users against impersonators by notifying users when someone else has uploaded a photo of them for use as a profile photo and to enable features on the service to people who are visually impaired. Facebook also uses facial-recognition technology to suggest that people who upload photos or videos tag the people who appear in the photos or videos. When someone is tagged in a photo or video, Facebook automatically notifies that person that he or she has been tagged, which in turn enables that person to take action if he or she does not like the content—such as removing the tag or requesting that the content be removed entirely. Facebook users have always had the ability to change their settings to prevent Facebook from using facial recognition to recognize them.

Given the very different uses of facial-recognition technology that exist, we believe that a one-size-fits-all approach to regulation of facial-recognition technology is not in the public's best interest, and we believe that clarification that the Illinois Biometric Information Privacy Act was not intended to apply to all uses of facial recognition is consistent with Facebook's commitment to protecting privacy. Furthermore, our commitment to support meaningful, thoughtfully drafted privacy legislation means that we can and do oppose measures that create confusion, interfere with legitimate law enforcement action, create unnecessary risk of frivolous litigation, or place undue burdens on people's ability to do business online.

Chairman THUNE. Thank you, Senator Durbin.
Senator Cornyn.

STATEMENT OF HON. JOHN CORNYN,
U.S. SENATOR FROM TEXAS

Senator CORNYN. Thank you, Mr. Zuckerberg, for being here.

I note that up until 2014 the mantra or motto of Facebook was "move fast and break things." Is that correct?

Mr. ZUCKERBERG. I do not know when we changed it, but the mantra is currently "move fast with stable infrastructure," which is a much less sexy mantra.

Senator CORNYN. It sounds much more boring, but my question is during the time that it was Facebook's mantra or motto to move fast and break things, do you think some of the misjudgments, perhaps mistakes that you have admitted to here were as a result of that culture or that attitude, particularly as regards to personal privacy, the information of your subscribers?

Mr. ZUCKERBERG. Senator, I do think that we made mistakes because of that, but the broadest mistakes that we made here are not taking a broad enough view of our responsibility. And while that was not a matter—the "move fast" cultural value is more tactical around whether engineers can ship things and different ways that we operate, but I think the big mistake that we have made looking back on this is viewing our responsibility as just building tools rather than viewing our whole responsibility as making sure that those tools are used for good.

Senator CORNYN. Well, and I appreciate that because previously or in the past we have been told that platforms like Facebook, Twitter, Instagram, and the like are neutral platforms and the people who own and run those for profit—and I am not criticizing doing something for profit in this country—but they bore no responsibility for the content. You agree now that Facebook and other social media platforms are not neutral platforms but bear some responsibility for the content?

Mr. ZUCKERBERG. I agree that we are responsible for the content. And I think that there is—one of the big societal questions that I think we are going to need to answer is the current framework that we have is based on this reactive model that assumed that there weren't AI tools that can proactively tell whether something was terrorist content or something bad, so it naturally relied on requiring people to flag for a company and then the company needed to take reasonable action.

In the future, we are going to have tools that are going to be able to identify more types of bad content, and I think that there are moral and legal obligation questions that I think we will have to

wrestle with as a society about when we want to require companies to take action proactively on certain of those things——

Senator CORNYN. I——

Mr. ZUCKERBERG.—and when that gets in the way of——

Senator CORNYN. I appreciate that. I have two minutes left——

Mr. ZUCKERBERG. All right.

Senator CORNYN.—to ask you questions. So, interestingly, the terms of the—what do you call it? The terms of service is a legal document which discloses to your subscribers how their information is going to be used, how Facebook is going to operate. But you concede that you doubt everybody reads or understands that legalese, those terms of service. So is that to suggest that the consent that people give, subject to that terms of services, is not informed consent? In other words, they may not read it, and even if they read it, they may not understand it.

Mr. ZUCKERBERG. I just think we have a broader responsibility than what the law requires, so I think we need to——

Senator CORNYN. No, I appreciate that. What I am asking about in terms of what your subscribers understand in terms of how their data is going to be used. But let me go to the terms of service under paragraph number two, you say you own all of the content and information you post on Facebook. That is what you have told us here today a number of times. So if I choose to terminate my Facebook account, can I bar Facebook or any third parties from using the data that I had previously supplied for any purpose whatsoever?

Mr. ZUCKERBERG. Yes, Senator. If you delete your account, we should get rid of all of your information.

Senator CORNYN. You should or——

Mr. ZUCKERBERG. We do.

Senator CORNYN.—do you?

Mr. ZUCKERBERG. We do.

Senator CORNYN. How about third parties that you have contracted with who use some of that underlying information perhaps to target advertising for themselves? Do you claw back that information as well, or does that remain in their custody?

Mr. ZUCKERBERG. Well, Senator, this is actually a very important question, and I am glad you brought this up because there is a very common misperception about Facebook that we sell data to advertisers, and we do not sell data to advertisers. We do not sell data to anyone.

Senator CORNYN. Well, you clearly rent it.

Mr. ZUCKERBERG. What we allow is for advertisers to tell us who they want to reach, and then we do the placement. So if an advertiser comes to us and says, all right, I am a ski shop and I want to sell skis to women, then we might have some sense because people shared skiing-related content or said they were interested in that. They shared whether they are a woman, and then we can show the ads to the right people without that data ever changing hands and going to the advertiser. That is a very fundamental part of how our model works and something that is often misunderstood, so I appreciate that you brought that up.

Chairman THUNE. Thank you, Senator Cornyn.

We had indicated earlier on that we would take a couple of breaks and give our witness an opportunity, and I think we have been going now for just under 2 hours, so I think what we will do, Mr. Zuckerberg.

Mr. ZUCKERBERG. We can do a few more.

[Laughter.]

Chairman THUNE. You want to keep going?

Mr. ZUCKERBERG. Maybe 15 minutes.

Chairman THUNE. OK.

Mr. ZUCKERBERG. Does that work?

Chairman THUNE. All right. We will keep going. Senator Blumenthal is up next, and we will commence.

STATEMENT OF HON. RICHARD BLUMENTHAL,
U.S. SENATOR FROM CONNECTICUT

Senator BLUMENTHAL. Thank you, Mr. Chairman.

Thank you for being here today, Mr. Zuckerberg. You have told us today and you have told the world that Facebook was deceived by Aleksandr Kogan when he sold user information to Cambridge Analytica, correct?

Mr. ZUCKERBERG. Yes.

Senator BLUMENTHAL. I want to show you the terms of service that Aleksandr Kogan provided to Facebook and note for you that in fact Facebook was on notice that he could sell that user information. Have you seen these terms of service before?

Mr. ZUCKERBERG. I have not.

Senator BLUMENTHAL. Who in Facebook was responsible for seeing those terms of service that put you on notice that that information could be sold?

Mr. ZUCKERBERG. Senator, our app review team would be responsible for that. And——

Senator BLUMENTHAL. Has anyone been fired on that app review team?

Mr. ZUCKERBERG. Senator, not because of this.

Senator BLUMENTHAL. Does that term of service not conflict with the FTC order that Facebook was under at that very time that this term of service was in fact provided to Facebook? And you will note that the FTC order specifically requires Facebook to protect privacy. Is there not a conflict there?

Mr. ZUCKERBERG. Senator, it certainly appears that we should have been aware that this app developer submitted a term that was in conflict with the rules of the platform.

Senator BLUMENTHAL. Well, what happened here was in effect willful blindness. It was heedless and reckless, which in fact amounted to a violation of the FTC Consent Decree. Would you agree?

Mr. ZUCKERBERG. No, Senator. My understanding is not that this was a violation of the consent decree. But, as I have said a number of times today, I think we need to take a broader view of our responsibility around privacy than just what is mandated in the current laws and the consent——

Senator BLUMENTHAL. Well, here is my reservation, Mr. Zuckerberg, and I apologize for interrupting you, but my time is limited. We have seen the apology tours before. You have refused

to acknowledge even an ethical obligation to have reported this violation of the FTC consent decree. And we have letters, we have had contacts with Facebook employees, and I am going to submit a letter for the record from Sandy Parakilas, with your permission, that indicates not only a lack of resources but lack of attention to privacy.

[The information referred to follows:]

Dear Senator Blumenthal,

In 2011 and 2012, I led the team responsible for overseeing Facebook's data policy enforcement efforts governing third-party application developers who were using Facebook's App Platform, and responding to violations of that policy.

In my first week on the job, I was told about a troubling feature of the App Platform: there was no way to track the use of data after it left Facebook's servers. That is, once Facebook transferred user data to the developer, Facebook lost all insight into or control over it. To prevent abuse, Facebook created a set of platform policies that forbade certain kinds of activity, such as selling the data or passing it to an ad network or data broker such as Cambridge Analytica.

Facebook had the following tools to deal with developers who abused the platform policies: it could call the developer and demand answers; it could demand an audit of the developer's application and associated data storage, a right granted in the platform policies; it could ban the developer from the platform; it could sue the developer for breach of the policies; or it could do some combination of the above. During my sixteen months at Facebook, I called many developers and demanded compliance, but I don't recall the company conducting a single audit of a developer where the company inspected the developer's data storage. Lawsuits and outright bans for data policy violations were also very rare.

Despite the fact that executives at Facebook were well aware that developers could, without detection, pass data to unauthorized fourth parties (such as what happened with Cambridge Analytica), little was done to protect users. A similar, well-publicized incident happened in 2010, where Facebook user IDs were passed by apps to a company called Rapleaf, which was a data broker. Despite my attempts to raise awareness about this issue, nothing was done to close the vulnerability. It was difficult to get any engineering resources assigned to build or maintain critical features to protect users.

Unfortunately, Facebook's failure to address this clear weakness, during my time there or after I left, led to Cambridge Analytica's misappropriation of tens of millions of Americans' data.

Sincerely,

SANDY PARAKILAS.

THISISYOURDIGITALLIFE APP

APPLICATION END USER TERMS AND CONDITIONS

1. The Parties: This Agreement ("Agreement") is between Global Science Research ("We", "Us" or "GSR"), which is a research organisation registered in England and Wales (Number: 9060785) with its registered office based at St John's Innovation Centre, Cowley Road, Cambridge, CB4 0WS, and the User of the Application ("You" or "User").

2. Agreement to Terms: By using THISISYOURDIGITALLIF APP ("Application"), by clicking "OKAY" or by accepting any payment, compensation, remuneration or any other valid consideration, you consent to using the Application, you consent to sharing information about you with us and you also accept to be bound by the Terms contained herein.

3. Purpose of the Application: We use this Application to (a) provide people an opportunity to see their predicted personalities based on their Facebook information, and (b) as part of our research on understanding how people's Facebook data can predict different aspects of their lives. Your contribution and data will help us better understand relationships between human psychology and online behaviour.

4. Data Security and Storage: Data security is very important to us. All data is stored on an encrypted server that is compliant with EU Directive 95/46/EC on the protection of individuals with regard to the processing of personal data.

5. Your Statutory Rights: Depending on the server location, your data may be stored within the United States or in the United Kingdom. If your data is stored in the United States, American laws will regulate your rights. If your data is stored

within the United Kingdom (UK), British and European Union laws will regulate how the data is processed, even if you live in the United States. Specifically, data protection and processing falls under a law called the Data Protection Act 1998. Under British and European Union law, you are considered to be a "Data Subject", which means you have certain legal rights. These rights include the ability to see what data is stored about you. Where data held in the EU is transferred to the United States, GSR will respect any safe harbour principles agreed between the United States Department of Commerce and the European Commission. The GSR Data Controller can be contacted by e-mail at info@globalscienceresearch.com.

6. Information Collected: We collect any information that you choose to share with us by using the Application. This may include, inter alia, the name, demographics, status updates and Facebook likes of your profile and of your network.

7. Intellectual Property Rights: If you click "OKAY" or otherwise use the Application or accept payment, you permit GSR to edit, copy, disseminate, publish, transfer, append or merge with other databases, sell, licence (by whatever means and on whatever terms) and archive your contribution and data. Specifically, agreement to these Terms also means you waive any copyright and other intellectual property rights in your data and contribution to GSR, and grant GSR an irrevocable, sublicenceable, assignable, non-exclusive, transferrable and worldwide license to use your data and contribution for any purpose. You acknowledge that any and all intellectual property rights and database rights held in your data or contribution that is acquired by GSR or the Application will vest with GSR and that you will not have any claim in copyright, contract or otherwise. Nothing in this Agreement shall inhibit, limit or restrict GSR's ability to exploit, assert, transfer or enforce any database rights or intellectual property rights anywhere in the world. You also agree not attempt to appropriate, assert claim to, restrict or encumber the rights held in, interfere with, deconstruct, discover, decompile, disassemble, reconstruct or otherwise reverse-engineer the Application, the data collected by the Application or any other GSR technology, algorithms, databases, methods, formulae, compositions, designs, source code, underlying ideas, file formats, programming interfaces, inventions and conceptions of inventions whether patentable or un-patentable.

8. Informed Consent: By signing this form, you indicate that you have read, understand, been informed about and agree to these Terms. You also are consenting to have your responses, opinions, likes, social network and other related data recorded and for the data collected from you to be used by GSR. If you do not understand these Terms, or if you do not agree to them, then we strongly advise that you do not continue, do not click "OKAY", do not use the Application and do not to collect any compensation from us.

9. Variation of Terms: You permit GSR to vary these Terms from time to time to comply with relevant legislation, for the protection of your privacy or for commercial reasons. If you choose to provide us with your e-mail address, notice of any variation will be sent to that e-mail address. If you do not provide us with an e-mail address, you waive your right to be notified of any variation of terms. 10. Rights of Third Parties: A person who is not a Party to this Agreement will not have any rights under or in connection with it.

- *Privacy Policy*
- *Powered by* **Global Science Research**

 St John's Innovation Centre, Cowley Road, Cambridge, CB4 0WS

E-mail: *info@globalscienceresearch.com*

GSRApp APPLICATION END USER TERMS AND CONDITIONS

1. The Parties: This Agreement ("Agreement") is between Global Science Research ("We", "Us" or "GSR"), which is a research organisation registered in England and Wales (Number: 9060785) with its registered office based at Magdelene College, Cambridge, UK CB3 0AG, and the User of the Application ("You" or "User").
2. Agreement to Terms: By using GSRApp APP ("Application"), by clicking "OKAY" or by accepting any payment, compensation, remuneration or any other valid consideration, you consent to using the Application, you consent to sharing information about you with us and you also accept to be bound by the Terms contained herein.
3. Purpose of the Application: We use this Application as part of our research on understanding how people's Facebook data can predict different aspects

of their lives. Your contribution and data will help us better understand relationships between human psychology and online behaviour.

4. Data Security and Storage: Data security is very important to us. All data is stored on an encrypted server that is compliant with EU Directive 95/46/EC on the protection of individuals with regard to the processing of personal data.
5. Your Statutory Rights: Depending on the server location, your data may be stored within the United States or in the United Kingdom. If your data is stored in the United States, American laws will regulate your rights. If your data is stored within the United Kingdom (UK), British and European Union laws will regulate how the data is processed, even if you live in the United States. Specifically, data protection and processing falls under a law called the Data Protection Act 1998. Under British and European Union law, you are considered to be a "Data Subject", which means you have certain legal rights. These rights include the ability to see what data is stored about you. Where data held in the EU is transferred to the United States, GSR will respect any safe harbour principles agreed between the United States Department of Commerce and the European Commission. The GSR Data Controller can be contacted by e-mail at alexbkogan@gmail.com.
6. Information Collected: We collect any information that you choose to share with us by using the Application. This may include, inter alia, the name, demographics, status updates and Facebook likes of your profile and of your network.
7. Intellectual Property Rights: If you click "OKAY" or otherwise use the Application or accept payment, you permit GSR to edit, copy, disseminate, publish, transfer, append or merge with other databases, sell, licence (by whatever means and on whatever terms) and archive your contribution and data. Specifically, agreement to these Terms also means you waive any copyright and other intellectual property rights in your data and contribution to GSR, and grant GSR an irrevocable, sublicenceable, assignable, non-exclusive, transferrable and worldwide license to use your data and contribution for any purpose. You acknowledge that any and all intellectual property rights and database rights held in your data or contribution that is acquired by GSR or the Application will vest with GSR and that you will not have any claim in copyright, contract or otherwise. Nothing in this Agreement shall inhibit, limit or restrict GSR's ability to exploit, assert, transfer or enforce any database rights or intellectual property rights anywhere in the world. You also agree not attempt to appropriate, assert claim to, restrict or encumber the rights held in, interfere with, deconstruct, discover, decompile, disassemble, reconstruct or otherwise reverse-engineer the Application, the data collected by the Application or any other GSR technology, algorithms, databases, methods, formulae, compositions, designs, source code, underlying ideas, file formats, programming interfaces, inventions and conceptions of inventions whether patentable or un-patentable.
8. Informed Consent: By signing this form, you indicate that you have read, understand, been informed about and agree to these Terms. You also are consenting to have your responses, opinions, likes, social network and other related data recorded and for the data collected from you to be used by GSR. If you do not understand these Terms, or if you do not agree to them, then we strongly advise that you do not continue, do not click "OKAY", do not use the Application and do not to collect any compensation from us.
9. Variation of Terms: You permit GSR to vary these Terms from time to time to comply with relevant legislation, for the protection of your privacy or for commercial reasons. If you choose to provide us with your e-mail address, notice of any variation will be sent to that e-mail address. If you do not provide us with an e-mail address, you waive your right to be notified of any variation of terms.
10. Rights of Third Parties: A person who is not a Party to this Agreement will not have any rights under or in connection with it.

Senator BLUMENTHAL. And so my reservation about your testimony today is that I do not see how you can change your business model unless there are specific rules of the road. Your business model is to monetize user information to maximize profit over privacy. And unless there are specific rules and requirements enforced

by an outside agency, I have no assurance that these kinds of vague commitments are going to produce action.

So I want to ask you a couple of very specific questions, and they are based on legislation that I have offered in the MY DATA Act and in legislation that Senator Markey is introducing today, the CONSENT Act, which I am joining. Do you not agree that companies ought to be required to provide users with clear, plain information about how their data will be used and specific ability to consent to the use of that information?

Mr. ZUCKERBERG. Senator, I do generally agree with what you are saying, and I laid that out earlier when I talked about what——

Senator BLUMENTHAL. Would you agree to an opt-in as opposed to an opt-out?

Mr. ZUCKERBERG. Senator, I think that that certainly makes sense to discuss, and I think the details around this matter a lot, so——

Senator BLUMENTHAL. Would you agree that users should be able to access all of their information?

Mr. ZUCKERBERG. Senator, yes, of course.

Senator BLUMENTHAL. All of the information that you collect as a result of purchases from data brokers, as well as tracking them?

Mr. ZUCKERBERG. Senator, we have already a download-your-information tool that allows people to see and to take out all of the information that they have put into Facebook or that Facebook knows about them. So yes, I agree with that. We already have that.

Senator BLUMENTHAL. I have a number of other specific requests that you agree to support as part of legislation. I think legislation is necessary. The rules of the road have to be the result of congressional action.

Facebook has participated recently in the fight against the scourge of sex trafficking, and the bill that we have just passed, it will be signed into law tomorrow, SESTA, the Stop Enabling Sex Trafficking Act, was the result of our cooperation. I hope that we can cooperate on this kind of measure as well.

Mr. ZUCKERBERG. Senator, I look forward to having my team work with you on this.

[The information referred to follows:]

I have a number of other specific requests that you agree to support as part of legislation. I think legislation is necessary. The rules of the road have to be the result of congressional action. We have—Facebook has participated recently in the fight against the scourge of sex trafficking and the bill that we've just passed. It will be signed into law tomorrow. The Stop Exploiting Sex Trafficking Act was as a result of our cooperation and I hope we can cooperate on this kind of measure as well.

Facebook supports SESTA, and we were very pleased to be able to work successfully with a bipartisan group of Senators on a bill that protects women and children from the harms of sex trafficking.

Facebook is generally not opposed to regulation but wants to ensure it is the right regulation. The issues facing the industry are complex, multi-faceted, and affect an important part of peoples' lives. As such, Facebook is absolutely committed to working with regulators, like Congress, to craft the right regulations. Facebook would be happy to review any proposed legislation and provide comments.

Senator BLUMENTHAL. Thank you.

Chairman THUNE. Thank you, Senator Blumenthal.

Senator Cruz.

STATEMENT OF HON. TED CRUZ,
U.S. SENATOR FROM TEXAS

Senator CRUZ. Thank you, Mr. Chairman.

Mr. Zuckerberg, welcome. Thank you for being here.

Mr. Zuckerberg, does Facebook consider itself a neutral public forum?

Mr. ZUCKERBERG. Senator, we consider ourselves to be a platform for all ideas.

Senator CRUZ. Let me ask the question again. Does Facebook consider itself to be a neutral public forum? And representatives of your company have given conflicting answers on this. Are you a First Amendment——

Mr. ZUCKERBERG. Well——

Senator CRUZ.—speaker expressing your views, or are you a neutral public forum allowing everyone to speak?

Mr. ZUCKERBERG. Senator, here is how we think about this. I do not believe that—there is certain content that clearly we do not allow, right? Hate speech, terrorist content, nudity, anything that makes people feel unsafe in the community. From that perspective, that is why we generally try to refer to what we do as a platform for——

Senator CRUZ. Let me try——

Mr. ZUCKERBERG.—all ideas——

Senator CRUZ.—this because the time is constrained. It is just a simple question. The predicate for Section 230 immunity under the CDA is that you are a neutral public forum. Do you consider yourself a neutral public forum or are you engaged in political speech, which is your right under the First Amendment?

Mr. ZUCKERBERG. Well, Senator, our goal is certainly not to engage in political speech. I am not that familiar with the specific legal language of the law that you speak to, so I would need to follow up with you on that. I am just trying to lay out how broadly I think about this.

[The information referred to follows:]

The predicate for Section 230 immunity under the CDA is that you're a neutral public forum. Do you consider yourself a neutral public forum or are you engaged in political speech, which is your right under the First Amendment?

We are, first and foremost, a technology company. Facebook does not create or edit the content that our users published on our platform. While we seek to be a platform for a broad range of ideas, we do moderate content in good faith according to published community standards in order to keep users on the platform safe, reduce objectionable content and to make sure users participate on the platform responsibly.

Section 230 of the Communications Decency Act provides that "[N]o provider or user of an interactive computer service shall be treated as the publisher or speaker of any information provided by another information content provider." Outside of certain specific exceptions, this means that online platforms that host content posted by others are generally not liable for the speech of their users, and, indeed, Section 230 explicitly provides that a platform that chooses to moderate content on its service *based on its own standards* does not incur liability on the basis of that decision. Specifically, 47 U.S.C. § 230(c)(2) provides, in relevant part, that "[N]o provider or user of an interactive computer service shall be held liable on account of—(A) any action voluntarily taken in good faith to restrict access to or availability of material that the provider or user considers to be obscene, lewd, lascivious, filthy, excessively violent, harassing, or otherwise objectionable, whether or not such material is constitutionally protected."

Senator CRUZ. Well, Mr. Zuckerberg, I will say there are a great many Americans who I think are deeply concerned that Facebook and other tech companies are engaged in a pervasive pattern of bias and political censorship. There have been numerous instances with Facebook. In May of 2016, Gizmodo reported that Facebook had purposefully and routinely suppressed conservative stories from trending news, including stories about CPAC, including stories about Mitt Romney, including stories about the Lois Lerner IRS scandal, including stories about Glenn Beck.

In addition to that, Facebook has initially shut down the Chick-fil-A Appreciation Day page, has blocked a post of a Fox News reporter, has blocked over two dozen Catholic pages, and most recently blocked Trump supporters Diamond and Silk page with 1.2 million Facebook followers after determining their content and brand were, quote, "unsafe to the community." To a great many Americans, that appears to be a pervasive pattern of political bias. Do you agree with that assessment?

Mr. ZUCKERBERG. Senator, let me say a few things about this. First, I understand where that concern is coming from because Facebook and the tech industry are located in Silicon Valley, which is an extremely left-leaning place. And this is actually a concern that I have and that I try to root out in the company is making sure that we do not have any bias in the work that we do. And I think it is a fair concern that people would at least wonder about.

Senator CRUZ. So let me ask this question.

Mr. ZUCKERBERG. Now——

Senator CRUZ. Are you aware of any ad or page that has been taken down from Planned Parenthood?

Mr. ZUCKERBERG. Senator, I am not, but let me just—can I——

Senator CRUZ. How about MoveOn.org?

Mr. ZUCKERBERG.—finish? I am sorry.

Senator CRUZ. How about MoveOn.org?

Mr. ZUCKERBERG. I am not specifically aware of those instances.

Senator CRUZ. How about any democratic candidate for office?

Mr. ZUCKERBERG. I am not specifically aware. I mean, I am not sure.

Senator CRUZ. In your testimony you say that you have 15,000 to 20,000 people working on security and content review. Do you know the political orientation of those 15,000 to 20,000 people engaged in content review?

Mr. ZUCKERBERG. No, Senator. We do not generally ask people about their political orientation when they are joining the company.

Senator CRUZ. So, as CEO, have you ever made hiring or firing decisions based on political positions or what candidates they supported?

Mr. ZUCKERBERG. No.

Senator CRUZ. Why was Palmer Luckey fired?

Mr. ZUCKERBERG. That is a specific personnel matter. That seems like it would be inappropriate to speak to here.

Senator CRUZ. You just made a specific representation that you did not make decisions based on political views. Is that accurate?

Mr. ZUCKERBERG. Well, I can commit that it was not because of a political view.

Senator CRUZ. Do you know of those 15,000 to 20,000 people engaged in content review how many if any have ever supported financially a Republican candidate for office?

Mr. ZUCKERBERG. Senator, I do not know that.

Senator CRUZ. Your testimony says, "It is not enough that we just connect people; we have to make sure those connections are positive." It says, "We have to make sure people are not using their voice to hurt people or spread misinformation. We have a responsibility not just to build tools but to make sure those tools are used for good." Mr. Zuckerberg, do you feel it is your responsibility to assess users, whether they are good and positive connections or ones that those 15,000 to 20,000 people deem unacceptable or deplorable?

Mr. ZUCKERBERG. Senator, you are asking about me personally?

Senator CRUZ. Facebook.

Mr. ZUCKERBERG. Senator, I think that there are a number of things that we would all agree are clearly bad. Foreign interference in our elections, terrorism, self-harm, those are things——

Senator CRUZ. I am talking about censorship.

Mr. ZUCKERBERG. Oh, well, I think that you would probably agree that we should remove terrorist propaganda from the service. So that I agree I think is clearly bad activity that we want to get down, and we are generally proud of how well we do with that.

Now, what I can say—and I do want to get this in before the end here—is that I am very committed to making sure that Facebook is a platform for all ideas. That is a very important founding principle of what we do. We are proud of the discourse and the different ideas that people can share on the service, and that is something that, as long as I am running the company, I am going to be committed to making sure is the case.

Senator CRUZ. Thank you.

Chairman THUNE. Thank you, Senator Cruz. Do you want to break now?

[Laughter.]

Chairman THUNE. Or do you want to keep going?

[Laughter.]

Mr. ZUCKERBERG. Sure. I mean, that was pretty good, so—all right.

[Laughter.]

Chairman THUNE. All right. Senator Whitehouse is up next, but if you want to take a——

Mr. ZUCKERBERG. Yes.

Chairman THUNE.—five-minute break right now, we have now been going a good 2 hours so——

Mr. ZUCKERBERG. Thank you.

Chairman THUNE.—we will recess for 5 minutes and reconvene.

[Recess.]

Chairman GRASSLEY [presiding]. The Committee will come to order.

Before I call on Senator Whitehouse, Senator Feinstein asked permission to put letters and statements in the record. And without objection, they will be put in from the ACLU, the Electronic Privacy Information Center, the Association for Computing Machinery Public Policy Council, and Public Knowledge.

[The information referred to follows:]

AMERICAN CIVIL LIBERTIES UNION
Washington, DC, April 9, 2018

Re: Questions for Mark Zuckerberg

Dear Senator,

On behalf of the American Civil Liberties Union ("ACLU"), we submit this letter for the record in connection with the Senate Judiciary and Commerce, Science, and Transportation Committees joint hearing, "Facebook, Social Media Privacy, and the Use and Abuse of Data," where Facebook Chairman and Chief Executive Officer Mark Zuckerberg is scheduled to testify.

Over the last month, the public has learned of various privacy breaches that have impacted tens of millions of Facebook users. The personal information of as many as 87 million people may have been improperly shared with Cambridge Analytica, which appears to have used this data to influence American voters.[1] Most Facebook users have reportedly had their public profile scraped for malicious purposes.[2] And, Facebook is currently being sued over concerns that it continues to fail to prevent ads that appear on the platform from improperly discriminating on the basis of gender, age, and other protected characteristics.[3] These incidents highlight both the existence of systemic deficiencies within Facebook and the need for stronger privacy laws in the U.S. to protect consumers.

We anticipate that members will question Mr. Zuckerberg regarding the recent incidents, the reasons Facebook has failed to adequately protect user privacy, and regulatory proposals the company will support. In addition to these topics, we urge you to ask Mr. Zuckerberg the following questions:

- Why has Facebook failed to take sufficient steps to ensure that advertisers do not wrongly exclude individuals from housing, employment, credit, and public accommodation ads based on gender, ethnic affinity, age, or other protected characteristics?
- Will Facebook provide privacy protections related to consent, retention, data portability, and transparency to American consumers that it will provide to EU consumers as a result of Europe's law on data protection, the General Data Protection Regulation ("GDPR"),[4] which will go into effect on May 25, 2018? In short, does Facebook plan to offer better privacy protection to Europeans than it does to Americans?

1. Facebook Ad Discrimination

Facebook offers advertisers many thousands of targeting categories, including those based on characteristics that are protected by civil rights laws—such as, gender, age, familial status, sexual orientation, disability, and veteran status—and those based on "proxies" for such characteristics. In the case of ads for housing, credit, and employment, discriminatory ad targeting and exclusion is illegal. Even outside these contexts, however, discriminatory targeting could raise civil rights concerns. For example, do we want any advertisers to be able to offer higher prices to individuals who Facebook believes are a particular race, or to exclude them from receiving ads offering certain commercial benefits?

Following complaints of discriminatory targeting, including efforts by the ACLU to raise concerns directly with the company, Facebook announced that it would no longer allow housing, credit, and employment ads targeted based on "affinity" for

---

[1] Kurt Wagner, *Facebook says Cambridge Analytica may have had data from as many as 87 million people,* RECODE, April 4, 2018, *https://www.recode.net/2018/4/4/17199272/facebook-cambridge-analytica-87-million-users-data-collection* (last visited Apr 5, 2018).

[2] Tony Romm, Craig Timberg & Elizabeth Dwoskin, *Malicious Actors' used its tools to discover identities and collect data on a massive global scale,* WASHINGTON POST, April 5, 2018, *https://www.washingtonpost.com/news/the-switch/wp/2018/04/04/facebook-said-the-personal-data-of-most-its-2-billion-users-has-been-collected-and-shared-with-outsiders/?utm_term=.31c3a8a679ee* (last visited Apr 5, 2018).

[3] Charles Baglie, *Facebook Vowed to End Discriminatory Housing Ads. Suits Says it Didn't.,* NEW YORK TIMES, March 27, 2018, available at *https://www.nytimes.com/2018/03/27/nyregion/facebook-housing-ads-discrimination-lawsuit.html* (last visited Apr 5, 2018).

[4] *Regulation (EU) 2016/679 of the European Parliament and Council of the European Union on the Protection of Natural Persons with Regard to the Processing of Personal Data and on the Free Movement of Such Data, and Repealing Directive 95/46/EC (General Data Protection Regulation)* [hereinafter GDPR], April 27, 2016, available at *http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679&qid=1490179745294&from=en*

certain ethnic groups.[5] However, it did not prohibit targeting based on gender, age, veteran status, or other protected categories.

These changes also did not address questions or concerns surrounding intentional targeting or exclusion of ads for public accommodations (for example, transportation). However, even after Facebook announced that it would no longer allow targeting of certain ads based on ethnic affinity, a ProPublica study found that the platform still failed to catch and prevent discriminatory ads that improperly excluded categories of users under the guise of targeting based on interests or affinity, including African Americans, Jewish people, and Spanish speakers.[6] Since then, Facebook has temporarily turned off ad targeting based on ethnic affinity until it can address these issues.[7]

Members should ask Zuckerberg why the platform has not turned off ad targeting for all protected categories or their proxies in the housing, credit, and employment, given that existing civil rights laws prohibit discriminatory ads in these contexts. In addition, they should question Zuckerberg regarding why the company has not taken sufficient steps—including increased auditing and facilitating research from independent entities—to assess and protect against discrimination outside of these contexts.

2. Privacy Protections Under the GDPR

For years, the ACLU has called on Facebook to provide more privacy protections to consumers and has emphasized the need for baseline privacy legislation in the U.S. With regards to Facebook, among other things, we have urged increased transparency, requirements that customers provide affirmative opt-in consent to share, use, or retain information, enhanced app privacy settings, auditing to assess third parties with access to Facebook, and other reforms. Many of these reforms have not been fully adopted, even in the wake of the Cambridge Analytica incident.[8]

However, some of these changes may soon be required for Facebook's operation in the European Union as a result of Europe's law on data protection, the GDPR, which will go into effect on May 25. The GDPR does not provide an exact template for what baseline privacy regulation should look like in the U.S.—indeed, provisions such as the right to be forgotten would likely be unconstitutional if applied in the U.S. Nevertheless, there are elements of the GDPR that, if applied in the U.S., would help to ensure that Americans have full control over their data and are equipped with the tools necessary to safeguard their rights.

In recent statements, Zuckerberg has said that Facebook is working to extend a version of the GDPR that could be extended globally, but has failed to provide details regarding which provisions of the law will be applied to U.S. consumers.[9] Given this, members of Congress should press Zuckerberg on whether Facebook intends to voluntarily provide certain GDPR protections[10] to U.S. consumers, including:

- *Consent Requirements:* Absent certain exceptions,[11] the GDPR requires that companies obtain user consent to collect, use, or otherwise process their per-

---

[5] Erin Egan, *Improving Enforcement and Promoting Diversity: Updates to Ethnic Affinity Marketing,* FACEBOOK, Nov. 11, 2016, *https://newsroom.fb.com/news/2016/11/updates-to-ethnic-affinity-marketing/* (last visited Apr 6, 2018).

[6] Julia Angwin, Ariana Tobin & Madeleine Varner, *Facebook (Still) Letting Housing Advertisers Exclude Users by Race, ProPublica,* PROPUBLICA, November 21, 2017, *https://www.propublica.org/article/facebook-advertising-discrimination-housing-race-sex-national-origin* (last visited Apr 5, 2018).

[7] Jessica Guynn, *Facebook halts ads that exclude racial and ethnic groups,* USA TODAY, Nov. 29, 2017, *https://www.usatoday.com/story/tech/2017/11/29/facebook-stop-allowing-advertisers-exclude-racial-and-ethnic-groups-targeting/905133001/* (last visited Apr 6, 2018).

[8] Nicole Ozer & Chris Conley, *https://www.aclu.org/blog/privacy-technology/internet-privacy/after-facebook-privacy-debacle-its-time-clear-steps-protect,* ACLU, Mar. 23, 2018, *https://www.aclu.org/blog/privacy-technology/internet-privacy/after-facebook-privacy-debacle-its-time-clear-steps-protect* (last visited Apr 6, 2018).

[9] David Ingrem & Joseph Menn, *Exclusive: Facebook CEO stops short of extending European privacy globally,* REUTERS, Apr. 3, 2018, *https://www.reuters.com/article/us-facebook-ceo-privacy-exclusive/exclusive-facebook-ceo-stops-short-of-extending-european-privacy-globally-idUSKCN1HA2M1* (last visited Apr 6, 2018).

[10] GDPR places different restrictions on entities based on whether they are "controllers" or "processors" of data. Facebook has stated that it acts as a controller for the majority of its business practices, though acts as a processor in certain instances when "working with business and third parties." For purposes of this letter, we have included obligations on Facebook as both a controller and processor. *See What is the General Data Protection Regulation,* Facebook Business, available at *https://www.facebook.com/business/gdpr.*

[11] Other than consent, a company may process data to fulfill a contractual obligation to which the user is a party or to take steps at the request of the user prior to a contract; to comply with a legal obligation, to perform a task in the public interest; to protect the vital interests

sonal data.[12] This consent must be freely given, specific, informed, and made by an affirmative action or statement by the user, and authorized by a parent/guardian if the user is under age 16.[13] If consent is written, the company must present the information in a manner that is intelligible, easily accessible, and uses clear and plain language. In addition, the user must have the right to withdraw their consent at any time.[14] In addition, processing of certain categories of sensitive data, like biometrics, religious beliefs, health data, and political opinions requires more rigorous "explicit consent."

- *Data Portability:* GDPR provides users the right to obtain a copy of the data they have provided in a "structured, commonly used and machine-readable format" and to have this data transferred to another provider.[15]
- *Transparency:* GDPR states that companies collecting data must provide transparency regarding their data processes. Among other things, users are entitled to know the amount of time their personal data will be stored (or the criteria used to determine the retention period), categories of personal data collected, whether the provision of the data is a statutory or contractual requirement, the existence of automated decision making, who receives their personal data, and the purpose for which their personal data is being collected, used, or otherwise processed.[16] There are also similar transparency requirements in cases where an entity obtains personal data about an individual from a source other than the individual.[17]
- *Use of Data for Marketing:* GDPR provides user the right to object to use of their data for marking purposes, including profiling for direct marketing purposes.[18]
- *Automated Decision-Making:* Absent certain exceptions (for example, explicit consent), GDPR states that users have the right to not be subject to decisions based solely on automated processing, including profiling, if it has a legal or similarly significant effect.[19]
- *Breach Notification:* In cases of any personal data breach, companies must notify a user if it is likely to result in a "high risk to the rights and freedoms" of individuals.[20] While the ACLU believes that notification should be required in circumstances far broader than this—and there are state laws that require notice in any case where there is a breach involving certain types of personal data[21]—the GDPR breach policy could be a step forward in cases where there is not more protective applicable U.S. law.

Voluntary application of GDPR requirements by companies to U.S. consumers cannot be a substitute for baseline privacy legislation in the U.S., which must include enforcement mechanisms, redress in the case of breaches, and a private right of action not subject to mandatory arbitration. Until such legislation, however, voluntary application of these rights could help to safeguard users in the U.S.

If you have questions, please contact ACLU Legislative Counsel, Neema Singh Guliani, at *nguliani@aclu.org.*

Sincerely,

FAIZ SHAKIR,
National Political Director.
NEEMA SINGH GULIANI,
Legislative Counsel.

---

of a data subject or other person; or to pursue a legitimate interest unless the interests are overridden by the interests/rights of the data subject. *See* GDRP, *supra* note 4, art. 6.

[12] *Id.*

[13] *Id.* at art. 4. GDPR permits members states to provide a lower age, no younger than 13, for consent purposes. *See Id.* at art. 6.

[14] *Id.* at art.7.

[15] *Id.* at art. 20.

[16] *Id.* at art. 12.

[17] *Id.* at art. 14.

[18] *Id.* at art. 21.

[19] *Id.* at art. 22.

[20] *Id.* at art. 34.

[21] *See* California Civ. Code s. 1798.82(a).

ELECTRONIC PRIVACY INFORMATION CENTER
Washington, DC, April 9, 2018

Senator CHUCK GRASSLEY, Chairman,
Senator DIANNE FEINSTEIN, Ranking Member,
Committee on the Judiciary,
Washington, DC.

Senator JOHN THUNE, Chairman,
Senator BILL NELSON, Ranking Members,
Committee on Commerce, Science, and Transportation,
Washington, DC.

Dear Members of the Senate Judiciary Committee and the Senate Commerce Committee:

We write to you regarding the joint hearing this week on "Facebook, Social Media Privacy, and the Use and Abuse of Data."[1] We appreciate your interest in this important issue. For many years, the Electronic Privacy Information Center ("EPIC") has worked with both the Judiciary Committee and the Commerce Committee to help protect the privacy rights of Americans.[2]

In this statement from EPIC, we outline the history of Facebook's 2011 Consent Order with the Federal Trade Commission, point to key developments (including the failure of the FTC to enforce the Order), and make a few preliminary recommendations. Our assessment is that the Cambridge Analytica breach, as well as a range of threats to consumer privacy and democratic institutions, could have been prevented if the Commission had enforced the Order.

EPIC would welcome the opportunity to testify, to provide more information, and to answer questions you may have. Our statement follows below.

EPIC, the 2011 FTC Consent Order, and Earlier Action by the FTC

Facebook's transfer of personal data to Cambridge Analytica was prohibited by a Consent Order the FTC reached with Facebook in 2011 in response to an extensive investigation and complaint pursued by EPIC and several U.S. consumer privacy organizations.[3] The FTC's failure to enforce the order we helped obtain has resulted in the unlawful transfer of 87 million user records to a controversial data mining firm to influence a presidential election as well as the vote in Brexit. The obvious question now is "why did the FTC fail to act?" The problems were well known, widely documented, and had produced a favorable legal judgement in 2011.

Back in 2007, Facebook launched Facebook Beacon, which allowed a Facebook user's purchases to be publicized on their friends' News Feed after transacting with third-party sites.[4] Users were unaware that such features were being tracked, and the privacy settings originally did not allow users to opt out. As a result of widespread criticism, Facebook Beacon was eventually shutdown.

In testimony before the Senate Commerce Committee in 2008, we warned about Facebook's data practices:

> Users of social networking sites are also exposed to the information collection practices of third party social networking applications. On Facebook, installing applications grants this third-party application provider access to nearly all of a user's information. Significantly, third party applications do not only access the information about a given user that has added the application. Applications by default get access to much of the information about that user's friends and

---

[1] *Facebook, Social Media Privacy, and the Use and Abuse of Data: Hearing Before the S. Comm. on the Judiciary,* 115th Cong. (2018), *https://www.judiciary.senate.gov/meetings/facebook-social-media-privacy-and-the-use-and-abuse-of-data* (April 10, 2018).

[2] *See, e.g., The Video Privacy Protection Act: Protecting Viewer Privacy in the 21st Century: Hearing Before the S. Comm on the Judiciary,* 112th Cong. (2012) (statement of Marc Rotenberg, Exec. Dir., EPIC), *https://epic.org/privacy/vppa/EPIC-Senate-VPPA-Testimony.pdf; An Examination of Children's Privacy: New Technologies and the Children's Online Privacy Protection Act (COPPA): Hearing Before the S. Comm. on Commerce, Science, and Transportation,* 111th Cong. (2010) (statement of Marc Rotenberg, Exec. Dir. EPIC), (C–SPAN video at *https://www.c-span.org/video/?293245–1/childrens-privacy*), *https://epic.org/privacy/kids/EPIC_COPPA_Testimony_042910.pdf; Impact and Policy Implications of Spyware on Consumers and Businesses: Hearing Before the S. Comm. on Commerce, Science, and Transportation* 110th Cong. (2008) (statement of Marc Rotenberg, Exec. Dir. EPIC) (C–SPAN video at *https://www.c-span.org/video/?205933-1/computer-spyware*), *https://www.epic.org/privacy/dv/Spyware_Test061108.pdf.*

[3] Fed. Trade Comm'n., *In re Facebook,* Decision and Order, FTC File No. 092 3184 (Jul. 27, 2012) (Hereinafter "Facebook Consent Order"), *https://www.ftc.gov/sites/default/files/documents/cases/2012/08/120810facebookdo.pdf.*

[4] EPIC, Social Networking Privacy, *https://epic.org/privacy/socialnet/.*

network members that the user can see. This level of access is often not necessary. Researchers at the University of Virginia found that 90 percent of applications are given more access privileges than they need.[5]

Nonetheless in February 2009, Facebook changed its Terms of Service. The new TOS allowed Facebook to use anything a user uploaded to the site for any purpose, at any time, even after the user ceased to use Facebook. Further, the TOS did not provide for a way that users could completely close their account. Rather, users could "deactivate" their account, but all the information would be retained by Facebook, rather than deleted.

EPIC planned to file an FTC complaint, alleging that the new Terms of Service violated the FTC Act Section 5, and constituted "unfair and deceptive trade practices." In response to this planned complaint, and a very important campaign organized by the "Facebook Users Against the New Terms of Service," Facebook returned to its previous Terms of Service. Facebook then established a comprehensive program of Governing Principles and a statement of Rights and Responsibilities.[6]

As we reported in 2009:

> Facebook has announced the results of the vote on site governance. The initial outcome indicates that approximately 75 percent of users voted for the new terms of service which includes the new Facebook Principles and Statement of Rights and Responsibilities. Under the new Principles, Facebook users will "own and control their information." Facebook also took steps to improve account deletion, to limit sublicenses, and to reduce data exchanges with application developers. EPIC supports the adoption of the new terms. For more information, see EPIC's page on Social Networking Privacy.[7]

However, Facebook failed to uphold its commitments to a public governance structure for the company.

From mid-2009 through 2011, EPIC and a coalition of consumer organizations pursued comprehensive accountability for the social media platform.[8] When Facebook broke its final commitment, we went ahead with a complaint to the Federal Trade Commission. Our complaint alleged that Facebook had changed user privacy settings and disclosed the personal data of users to third parties without the consent of users.[9] EPIC and others had conducted extensive research and documented the instances of Facebook overriding the users' privacy settings to reveal personal information and to disclose, for commercial benefit, user data, and the personal data of friends and family members, to third parties without their knowledge or affirmative consent.[10]

We explained our argument clearly in the 2009 EPIC complaint with the Commission (attached in full to this statement):

> This complaint concerns material changes to privacy settings made by Facebook, the largest social network service in the United States, which adversely impact users of the Facebook service. Facebook's changes to users' privacy settings disclose personal information to the public that was previously re-

---

[5] *Impact and Policy Implications of Spyware on Consumers and Businesses: Hearing Before the S. Comm. on Commerce, Science, and Transportation* 110th Cong. (2008) (statement of Marc Rotenberg, Exec. Dir. EPIC) (C–SPAN video at *https://www.c-span.org/video/?205933–1/computer-spyware*), *https://www.epic.org/privacy/dv/Spyware_Test061108.pdf.*

[6] *Facebook takes a Democratic Turn,* USA Today, Feb. 27, 2009, at 1B, *https://www.pressreader.com/usa/usa-today-us-edition/20090227/281887294213804*

[7] EPIC, *Facebook Gets Ready to Adopt Terms of Service* (Apr. 24, 2009) *https://epic.org/2009/04/facebook-gets-ready-to-adopt-t.html*

[8] There is a longer history of significant events concerning the efforts of Facebook users to establish democratic accountability for Facebook during the 2008–2009 period. The filing of the 2009 complaint came about after it became clear that Facebook would not uphold its commitments to the Statement of Right and Responsibilities it had established. It would also be worth reconstructing the history of the "Facebook Users Against the New Terms of Service" as Facebook destroyed the group and all records of its members and activities after the organizers helped lead a successful campaign against the company. Julius Harper was among the organizers of the campaign. A brief history was written by Ben Popken in 2009 for *The Consumerist,* "What Facebook's Users Want In The Next Terms Of Service," *https://consumerist.com/2009/02/23/what-facebooks-users-want-in-the-next-terms-of-service/*. Julius said this in 2012: "Most people on Facebook don't even know they can vote or even that a vote is going on. What is a democracy if you don't know where the polling place is? Or that a vote is even being held? How can you participate? Ignorance becomes a tool that can be used to disenfranchise people." *Facebook upsets some by seeking to take away users' voting rights,* San Jose Mercury News, Nov. 30, 2012, *https://www.mercurynews.com/2012/11/30/facebook-upsets-some-by-seeking-to-take-away-users-voting-rights/*.

[9] *In re Facebook,* EPIC.org, *https://epic.org/privacy/inrefacebook/*.

[10] *FTC Facebook Settlement,* EPIC.org, *https://epic.org/privacy/ftc/facebook/*.

> stricted. Facebook's changes to users' privacy settings also disclose personal information to third parties that was previously not available. These changes violate user expectations, diminish user privacy, and contradict Facebook's own representations. These business practices are Unfair and Deceptive Trade Practices, subject to review by the Federal Trade Commission (the "Commission") under section 5 of the Federal Trade Commission Act.[11]

We should also make clear that the 2009 complaint that EPIC filed with the Federal Trade Commission about Facebook was not the first to produce a significant outcome. In July and August 2001, EPIC and a coalition of fourteen leading consumer groups filed complaints with the Federal Trade Commission (FTC) alleging that the Microsoft Passport system violated Section 5 of the Federal Trade Commission Act (FTCA), which prohibits unfair or deceptive practices in trade.[12]

EPIC and the groups alleged that Microsoft violated the law by linking the Windows XP operating system to repeated exhortations to sign up for Passport; by representing that Passport protects privacy, when it and related services facilitate profiling, tracking and monitoring; by signing up Hotmail users for Passport without consent or even the ability to opt-out; by representing that the system complies with the Children's Online Privacy Protection Act; by not allowing individuals to delete their account; and by representing that the system securely holds individuals' data.

We requested that the FTC initiate an investigation into the information collection practices of Windows XP and other services, and to order Microsoft to revise XP registration procedures; to block the sharing of Passport information among Microsoft properties absent explicit consent; to allow users of Windows XP to gain access to Microsoft websites without disclosing their actual identity; and to enable users of Windows XP to easily integrate services provided by non-Microsoft companies for online payment, electronic commerce, and other Internet-based commercial activity.

The Federal Trade Commission undertook the investigation we requested and issued an important consent order. As the Commission explained announcing its enforcement action in 2002:

> Microsoft Corporation has agreed to settle Federal Trade Commission charges regarding the privacy and security of personal information collected from consumers through its "Passport" web services. As part of the settlement, Microsoft will implement a comprehensive information security program for Passport and similar services. . . .
>
> The Commission initiated its investigation of the Passport services following a July 2001 complaint from a coalition of consumer groups led by the Electronic Privacy Information Center (EPIC).
>
> According to the Commission's complaint, Microsoft falsely represented that:
>
> - It employs reasonable and appropriate measures under the circumstances to maintain and protect the privacy and confidentiality of consumers' personal information collected through its Passport and Passport Wallet services, including credit card numbers and billing information stored in Passport Wallet;
> - Purchases made with Passport Wallet are generally safer or more secure than purchases made at the same site without Passport Wallet when, in fact, most consumers received identical security at those sites regardless of whether they used Passport Wallet to complete their transactions;
> - Passport did not collect any personally identifiable information other than that described in its privacy policy when, in fact, Passport collected and held, for a limited time, a personally identifiable sign-in history for each user; and
> - The Kids Passport program provided parents control over what information participating Websites could collect from their children.
>
> The proposed consent order prohibits any misrepresentation of information practices in connection with Passport and other similar services. It also requires Microsoft to implement and maintain a comprehensive information security program. In addition, Microsoft must have its security program certified as meeting

---

[11] *In the Matter of Facebook, Inc.* (EPIC, Complaint, Request for Investigation, Injunction, and Other Relief) before the Federal Trade Commission, Washington, D.C. (filed Dec. 17, 2009), *http://www.epic.org/privacy/inrefacebook/EPIC-FacebookComplaint.pdf.*

[12] EPIC, *Microsoft Passport Investigation Docket, https://epic.org/privacy/consumer/microsoft/passport.html.*

> or exceeding the standards in the consent order by an independent professional every two years.[13]

FTC Chairmen Timothy J. Muris said at the time, "Good security is fundamental to protecting consumer privacy. Companies that promise to keep personal information secure must follow reasonable and appropriate measures to do so. It's not only good business, it's the law. Even absent known security breaches, we will not wait to act." [14]

Then in December 2004, EPIC filed a complaint with the Federal Trade Commission against databroker Choicepoint, urging the Commission to investigate the compilation and sale of personal dossiers by data brokers such as Choicepoint.[15] Based on the EPIC complaint, in 2005, the FTC charged that Choicepoint did not have reasonable procedures to screen and verify prospective businesses for lawful purposes and as a result compromised the personal financial records of more than 163,000 customers in its database. In January 2006, the FTC announced a settlement with Choicepoint, requiring the company to pay $10 million in civil penalties and provide $5 millions for consumer redress. EPIC's Choicepoint complaint produced the largest civil fine at the time in the history of the FTC.[16]

The Microsoft order led to user-centric identity scheme that, if broadly adopted, could have done much to preserve the original open, decentralized structure of the Internet. The Choicepoint order led to significant reforms in the data broker industry. And it is worth noting that both investigations were successfully pursued with Republican chairmen in charge of the Federal agency and both actions were based on unanimous decisions by all of the Commissioners.

The Facebook complaint should have produced an outcome even more consequential than the complaints concerning Microsoft and Choicepoint. In 2011, the FTC, based the materials we provided in 2009 and 2010, confirmed our findings and recommendations. In some areas, the FTC even went further. The FTC issued a Preliminary Order against Facebook in 2011 and then a Final Order in 2012.[17] In the press release accompanying the settlement, the FTC stated that Facebook "deceived consumers by telling them they could keep their information on Facebook private, and then repeatedly allowing it to be shared and made public." [18]

According to the FTC, under the proposed settlement Facebook is:

- "barred from making misrepresentations about the privacy or security of consumers' personal information;"
- "required to obtain consumers' affirmative express consent before enacting changes that override their privacy preferences;"
- "required to prevent anyone from accessing a user's material more than 30 days after the user has deleted his or her account;"
- "required to establish and maintain a comprehensive privacy program designed to address privacy risks associated with the development and management of new and existing products and services, and to protect the privacy and confidentiality of consumers' information; and"
- "required, within 180 days, and every two years after that for the next 20 years, to obtain independent, third-party audits certifying that it has a privacy program in place that meets or exceeds the requirements of the FTC order, and to ensure that the privacy of consumers' information is protected." [19]

The reporting requirements are set out in more detail in the text of the Final Order. According to the Final Order:

> [The] Respondent [Facebook] shall, no later than the date of service of this order, establish and implement, and thereafter maintain, a comprehensive pri-

---

[13] Fed. Trade Comm'n, *Microsoft Settles FTC Charges Alleging False Security and Privacy Promises: Passport Single Sign-In, Passport "Wallet," and Kids Passport Named in Complaint Allegations,* Press Release, (Aug. 8, 2002), *https://www.ftc.gov/news-events/press-releases/2002/08/microsoft-settles-ftc-charges-alleging-false-security-privacy.*

[14] *Id.*

[15] EPIC, ChoicePoint, *https://www.epic.org/privacy/choicepoint/*

[16] Fed. Trade Comm'n., *ChoicePoint Settles Data Security Breach Charges; to Pay $10 Million in Civil Penalties, $5 Million for Consumer Redress: At Least 800 Cases of Identity Theft Arose From Company's Data Breach* (Jan. 26, 2006), *https://www.ftc.gov/news-events/press-releases/2006/01/choicepoint-settles-data-security-breach-charges-pay-10-million.*

[17] Facebook Consent Order.

[18] Fed. Trade Comm'n., *Facebook Settles FTC Charges That It Deceived Consumers by Failing to Keep Privacy Promises,* Press Release, (Nov. 29, 2011), *https://www.ftc.gov/news-events/press-releases/2011/11/facebook-settles-ftc-charges-it-deceived-consumers-failing-keep.*

[19] *Id.*

vacy program that is reasonably designed to (1) address privacy risks related to the development and management of new and existing products and services for consumers, and (2) protect the privacy and confidentiality of covered information. Such program, the content and implementation of which must be documented in writing, shall contain controls and procedures appropriate to Respondent's size and complexity, the nature and scope of Respondent's activities, and the sensitivity of the covered information, including:

A. the designation of an employee or employees to coordinate and be responsible for the privacy program.

B. the identification of reasonably foreseeable, material risks, both internal and external, that could result in Respondent's unauthorized collection, use, or disclosure of covered information and an assessment of the sufficiency of any safeguards in place to control these risks. At a minimum, this privacy risk assessment should include consideration of risks in each area of relevant operation, including, but not limited to: (1) employee training and management, including training on the requirements of this order, and (2) product design, development, and research.

C. the design and implementation of reasonable controls and procedures to address the risks identified through the privacy risk assessment, and regular testing or monitoring of the effectiveness of those controls and procedures.

D. the development and use of reasonable steps to select and retain service providers capable of appropriately protecting the privacy of covered information they receive from Respondent and requiring service providers, by contract, to implement and maintain appropriate privacy protections for such covered information.

E. the evaluation and adjustment of Respondent's privacy program in light of the results of the testing and monitoring required by subpart C, any material changes to Respondent's operations or business arrangements, or any other circumstances that Respondent knows or has reason to know may have a material impact on the effectiveness of its privacy program.[20]

Moreover, the Final Order stated:

Respondent shall obtain initial and biennial assessments and reports ("Assessments") from a qualified, objective, independent third-party professional, who uses procedures and standards generally accepted in the profession. A person qualified to prepare such Assessments shall have a minimum of three (3) years of experience in the field of privacy and data protection. All persons selected to conduct such Assessments and prepare such reports shall be approved by the Associate Director for Enforcement, Bureau of Consumer Protection, Federal Trade Commission, Washington, D.C. 20580, in his or her sole discretion. Any decision not to approve a person selected to conduct such Assessments shall be accompanied by a writing setting forth in detail the reasons for denying such approval. The reporting period for the Assessments shall cover: (1) the first one hundred and eighty (180) days after service of the order for the initial Assessment, and (2) each two (2) year period thereafter for twenty (20) years after service of the order for the biennial Assessments. Each Assessment shall:

A. set forth the specific privacy controls that Respondent has implemented and maintained during the reporting period;

B. explain how such privacy controls are appropriate to Respondent's size and complexity, the nature and scope of Respondent's activities, and the sensitivity of the covered information;

C. explain how the privacy controls that have been implemented meet or exceed the protections required by Part IV of this order; and

D. certify that the privacy controls are operating with sufficient effectiveness to provide reasonable assurance to protect the privacy of covered information and that the controls have so operated throughout the reporting period.

Each Assessment shall be prepared and completed within sixty (60) days after the end of the reporting period to which the Assessment applies. Respondent shall provide the initial Assessment to the Associate Director for Enforcement, Bureau of Consumer Protection, Federal Trade Commission, Washington, D.C. 20580, within ten (10) days after the Assessment has been prepared. All subsequent biennial Assessments shall be retained by Respondent until the order is

[20] Facebook Consent Order.

terminated and provided to the Associate Director of Enforcement within ten (10) days of request.[21]

EPIC expressed support for the Consent Order but also believed it could be improved.[22] In response to the FTC's request for public comments on the proposed order we wrote:

> EPIC supports the findings in the FTC Complaint and supports, in part, the directives contained in the Consent Order. The Order makes clear that companies should not engage in unfair and deceptive trade practices, particularly in the collection and use of personal data. However, the proposed Order is insufficient to address the concerns originally identified by EPIC and the consumer coalition, as well as those findings established by the Commission. Consistent with this earlier determination, to protect the interests of Facebook users, and in light of recent changes in the company's business practices, EPIC urges the Commission to require Facebook to:
>
> - Restore the privacy settings that users had in 2009, before the unfair and deceptive practices addressed by the Complaint began;
> - Allow users to access all of the data that Facebook keeps about them;
> - Cease creating facial recognition profiles without users' affirmative consent;
> - Make Facebook's privacy audits publicly available to the greatest extent possible;
> - Cease secret post-log out tracking of users across websites.

At the time, the FTC settlement with Facebook was widely viewed as a major step forward for the protection of consumer privacy in the United States. The Chairman of the FTC stated, "Facebook is obligated to keep the promises about privacy that it makes to its hundreds of millions of users. Facebook's innovation does not have to come at the expense of consumer privacy. The FTC action will ensure it will not." Mark Zuckerberg said at the time of the Consent Order that the company had made "a bunch of mistakes."[23] The FTC Chair called Mr. Zuckerberg's post a "good sign" and said, "He admits mistakes. That can only be good for consumers."[24]

Commissioners and staff of the FTC later testified before Congress, citing the Facebook Consent Order as a major accomplishment for the Commission.[25] And U.S. policymakers held out the FTC's work in discussions with trading partners for the proposition that the U.S. could provide privacy protections to those users of US-

---

[21] *Id.* at 6–7.

[22] Comments of EPIC, *In the Matter of Facebook, Inc.,* FTC File No. 092 3184, (Dec. 27, 2011), *https://epic.org/privacy/facebook/Facebook-FTC-Settlement-Comments-FINAL.pdf.*

[23] Somini Sengupta, *F.T.C. Settles Privacy Issue at Facebook,* N.Y. Times, at B1 (Nov. 29, 2011), *https://www.nytimes.com/2011/11/30/technology/facebook-agrees-to-ftc-settlement-on-privacy.html.* There was also a "lengthy blog post" from Mr. Zuckerberg in the N.Y. Times article but the link no longer goes to Mr. Zuckerberg's original post. Mr. Zuckerberg's post in 2009 that established the Bill of Rights and Responsibilities for the site has also disappeared. This is the original link: *http://blog.facebook.com/blog.php?post=54746167130.*

[24] Julianne Pepitone, *Facebook settles FTC charges over 2009 privacy breaches,* CNN Money (Nov. 29, 2011), *http://money.cnn.com/2011/11/29/technology/facebook_settlement/index.htm.*

[25] According to the statement of the FTC Commissioners who testified before the Senate Commerce Committee in 2012:

> Similar to the Google order, the Commission's consent order against Facebook prohibits the company from deceiving consumers with regard to privacy; requires it to obtain users' affirmative express consent before sharing their information in a way that exceeds their privacy settings; and requires it to implement a comprehensive privacy program and obtain outside audits. In addition, Facebook must ensure that it will stop providing access to a user's information after she deletes that information.
>
> *The Need for Privacy Protections: Perspectives from the Administration and the Federal Trade Commission: Hearing Before the S. Comm on Commerce, Science and Transportation,* at 18, 112th Cong. (May 9, 2012) (statement of Fed. Trade Comm'n.), *https://www.ftc.gov/sites/default/files/documents/public_statements/prepared-statement-federal-trade-commission-need-privacy-protections-perspectives-administration-and/120509privacyprotections.pdf; see also, The Need for Privacy Protections: Perspectives from the Administration and the Federal Trade Commission, Hearing before the S. Comm. on Commerce, Science, and Transportation, 112th Cong. (May 19, 2012)* (statement of Maureen K. Ohlhausen, Commissioner, Fed. Trade Comm'n) ("We have also charged companies with failing to live up to their privacy promises, as in the highly publicized privacy cases against companies such as Google and Facebook, which together will protect the privacy of more than one billion users worldwide. As a Commissioner, I will urge continuation of this strong enforcement record."), *https://www.ftc.gov/sites/default/files/documents/public_statements/statement-commissioner-maureen-k.ohlhausen/120509privacytestimony.pdf.*

based services. For example, former FTC Chairwoman wrote this to Věra Jourová, Commissioner for Justice, Consumers and Gender Equality, European Commission:

> As part of its privacy and security enforcement program, the FTC has also sought to protect EU consumers by bringing enforcement actions that involved Safe Harbor violations. . . . Twenty-year consent orders require Google, Facebook, and Myspace to implement comprehensive privacy programs that must be reasonably designed to address privacy risks related to the development and management of new and existing products and services and to protect the privacy and confidentiality of personal information. The comprehensive privacy programs mandated under these orders must identify foreseeable material risks and have controls to address those risks. The companies must also submit to ongoing, independent assessments of their privacy programs, which must be provided to the FTC. The orders also prohibit these companies from misrepresenting their privacy practices and their participation in any privacy or security program. This prohibition would also apply to companies' acts and practices under the new Privacy Shield Framework. . . . Consequently, these FTC orders help protect over a billion consumers worldwide, hundreds of millions of whom reside in Europe.[26]

Yet the Federal Trade Commission never charged Facebook with a single violation of the 2011 Consent Order.

The Google Consent Order and the FTC's Subsequent Failure to Enforce Consent Orders

In 2011, we also had also obtained a significant consent order at the FTC against Google after the disastrous roll-out of Google "Buzz." In that case, the FTC established a consent order after Google tried to enroll Gmail users into a social networking service without meaningful consent. The outcome was disastrous. Personal contact information was made publicly available by Google as part of its effort to establish a social network service to compete with Facebook. EPIC filed a detailed complaint with the Commission in February that produced a consent order in 2011, comparable to the order for Facebook.[27]

But a problem we did not anticipate became apparent almost immediately: the Federal Trade Commission was unwilling to enforce its own consent orders. Almost immediately after the settlements, both Facebook and Google began to test the FTC's willingness to stand behind its judgements. Dramatic changes in the two companies' advertising models led to more invasive tracking of Internet users. Online and offline activities were increasingly becoming merged.

To EPIC and many others, these changes violated the terms of the consent orders. We urged the FTC to establish a process to review these changes and publish its findings so that the public could at least evaluate whether the companies were complying with the original orders. But the Commission remained silent, even as it claimed that its model was working well for these companies.

In 2012, EPIC sued the Commission when it became clear that Google was proposing to do precisely what the FTC said it could not—consolidate user data across various services that came with diverse privacy policies in order to build detailed individual profiles. The problem was widely understood. Many members of Congress in both parties, state attorneys general, and Jon Leibowitz, the head of the FTC itself, warned about the possible outcome. Even the federal court, which ruled that it could not require the agency to enforce its order, was sympathetic. "EPIC—along with many other individuals and organizations—has advanced serious concerns that may well be legitimate, and the FTC, which has advised the Court that the matter is under review, may ultimately decide to institute an enforcement action," wrote the judge.[28]

But that enforcement action never came. Even afterward, EPIC and other consumer privacy organizations have continued to urge the Federal Trade Commission

---

[26] Letter from FTC Chairwoman Edith Ramirez to Věra Jourová, Commissioner for Justice, Consumers and Gender Equality, European Commission, at 4–5 (Jul. 7, 2016), *https://www.privacyshield.gov/servlet/servlet.FileDownload?file=015t00000004q0v*

[27] *In the Matter of Google, Inc.,* EPIC Complaint, Request for Investigation, Injunction, and Other Relief, before the Federal Trade Commission, Washington, D.C. (filed Feb. 16, 2010), *https://epic.org/privacy/ftc/googlebuzz/GoogleBuzz_Complaint.pdf; Fed. Trade Comm'n., FTC Charges Deceptive Privacy Practices in Googles Rollout of Its Buzz Social Network: Google Agrees to Implement Comprehensive Privacy Program to Protect Consumer Data,* Press Release, (Mar. 30, 2011), *https://www.ftc.gov/news-events/press-releases/2011/03/ftc-charges-deceptive-privacy-practices-googles-rollout-its-buzz.*

[28] *EPIC v. FTC,* 844 F. Supp. 2d 98 (D.D.C. 2012), *https://epic.org/privacy/ftc/google/EPICvFTC-CtMemo.pdf.*

to enforce its consent orders. In our most recent comments to the Federal Trade Commissioner, we said simply "The FTC Must Enforce Existing Consent Orders." We wrote:

> The effectiveness of FTC enforcement is determined by the agency's willingness to enforce the legal judgments it obtains. The FTC should review substantial changes in business practices for companies under consent orders that implicate the privacy interests of consumers. Multiple prominent Internet firms have been permitted to alter business practices, without consequence, despite being subject to 20-year consent orders with the FTC. This has harmed consumers and promoted industry disregard for the FTC.[29]

The Senate Commerce Committee should be specifically concerned about the FTC's ongoing failure to enforce its consent orders. This agency practice poses an ongoing risk to both American consumers and American businesses.

Cambridge Analytica Breach

On March 16, 2018, Facebook admitted the unlawful transfer of 50 million user profiles to the data mining firm Cambridge Analytica, which harvested the data obtained without consent to influence the 2016 U.S. presidential election.[30] Relying on the data provided by Facebook, Cambridge Analytica was able to collect the private information of approximately 270,000 users and their extensive friend networks under false pretenses as a research-driven application.[31] Last week, Facebook announced that the number of users who had their data unlawfully harvested was actually closer to 87 million.[32]

This is in clear violation of the 2011 Consent Order, which states that Facebook "shall not misrepresent in any manner, expressly or by implication . . . the extent to which [Facebook] makes or has made covered information accessible to third parties; and the steps [Facebook] takes or has taken to verify the privacy or security protections that any third party provides."[33] Part II of the proposed order required Facebook to "give its users a *clear and prominent notice* and *obtain their affirmative express consent* before sharing their previously-collected information with third parties in any way that materially exceeds the restrictions imposed by their privacy settings."[34] Part IV "requires Facebook to *establish and maintain a comprehensive privacy program* that is reasonably designed to: (1) Address privacy risks related to the development and management of new and existing products and services, and (2) protect the privacy and confidentiality of covered information. The privacy program must be documented in writing and must contain controls and procedures appropriate to Facebook's size and complexity, the nature and scope of its activities, and the sensitivity of covered information."[35]

Response of EPIC and Consumer Privacy Organizations, Compliance with GDPR

After the news broke of the Cambridge Analytica breach, EPIC and a consumer coalition urged the FTC to reopen the Facebook investigation.[36] We stated, "Facebook's admission that it disclosed data to third parties without users' consent suggests a clear violation of the 2011 Facebook Order." We further said:

> The FTC has an obligation to the American public to ensure that companies comply with existing Consent Orders. It is unconscionable that the FTC allowed this unprecedented disclosure of Americans' personal data to occur. The FTC's failure to act imperils not only privacy but democracy as well.

---

[29] EPIC Statement to FTC (Feb. 2017), *https://epic.org/privacy/internet/ftc/EPIC-et-al-ltr-FTC-02-15-2017.pdf.*

[30] Press Release, Facebook, *Suspending Cambridge Analytica and SCL Group from Facebook* (Mar. 16, 2018), *https://newsroom.fb.com/news/2018/03/suspending-cambridge-analytica/*.

[31] *Id.*

[32] Cecilia Kang and Sheera Frenkel, *Facebook Says Cambridge Analytica Harvested Data of Up to 87 Million Users,* N.Y. Times, (Apr. 4, 2018), *https://www.nytimes.com/2018/04/04/technology/mark-*

[33] Federal Trade Commission, *Facebook, Inc.; Analysis of Proposed Consent Order To Aid Public Comment,* 76 Fed. Reg. 75883 (Dec. 5, 2011), *https://www.ftc.gov/sites/default/files/documents/federal_register_notices/facebook-inc.analysis-proposed-consent-order-aid-public-comment-proposed-consent-agreement/111205facebookfrn.pdf.*

[34] *Id.* (emphasis added).

[35] *Id.* (emphasis added).

[36] Letter to Acting Chairman Maureen Ohlhausen and Commissioner Terrell McSweeney from leading consumer privacy organizations in the United States (Mar. 20, 2018), *https://epic.org/privacy/facebook/EPIC-et-al-ltr-FTC-Cambridge-FB–03–20–18.pdf. See* "EPIC, Consumer Groups Urge FTC To Investigate Facebook" (Mar. 20, 2018), *https://epic.org/2018/03/epic-consumer-groups-urge-ftc-.html.*

On March 26, 2018, less than two weeks ago, the FTC announced it would reopen the investigation.[37] The Statement by the Acting Director of FTC's Bureau of Consumer Protection Regarding Reported Concerns about Facebook Privacy Practice, issued on March 26, 2018, was as follows:

> The FTC is firmly and fully committed to using all of its tools to protect the privacy of consumers. Foremost among these tools is enforcement action against companies that fail to honor their privacy promises, including to comply with Privacy Shield, or that engage in unfair acts that cause substantial injury to consumers in violation of the FTC Act. *Companies who have settled previous FTC actions must also comply with FTC order provisions imposing privacy and data security requirements.* Accordingly, the FTC takes very seriously recent press reports raising substantial concerns about the privacy practices of Facebook. Today, the FTC is confirming that it has an open non-public investigation into these practices.

Congress should monitor this matter closely. This may be one of the most consequential investigations currently underway in the Federal Government.

But others are not waiting for the resolution. State Attorneys General have also made clear their concerns about the Facebook matter.[38]

Also today, a broad coalition of consumer organizations in the United States and Europe, represented by the TransAtlantic Consumer Dialogue ("TACD"), will urge Mr. Zuckerberg to make clear his commitment to compliance with the General Data Protection Regulation. The TACD wrote:

> The GDPR helps ensure that companies such as yours operate in an accountable and transparent manner, subject to the rule of law and the democratic process. The GDPR provides a solid foundation for data protection, establishing clear responsibilities for companies that collect personal data and clear rights for users whose data is gathered. These are protections that all users should be entitled to no matter where they are located.[39]

EPIC supports the recommendation of TACD concerning the GDPR. There is little reason that a U.S. firm should provide better privacy protection to individuals outside the United States than it does to those inside our country.

Oversight of the Federal Trade Commission and Facebook Compliance with the 2011 Consent Order

Several former FTC commissioners and former FTC staff members have recently suggested that the FTC needs more authority to protect American consumers. At least with regard to enforcement of its current legal authority, we strongly disagree. The FTC could have done far more than it did.

On March 20, 2018, EPIC submitted a request to the FTC under the Freedom of Information Act for the 2013, 2015, and 2017 Facebook Assessments, as well as all records concerning the person(s) approved by the FTC to undertake the Facebook Assessments; and all records of communications between the FTC and Facebook regarding the Facebook Assessments. In 2013, EPIC received redacted version of Facebook's initial compliance report and first independent assessment after a similar FOIA request.[40]

Under the Final Consent Order, Facebook's initial assessment was due to the FTC on April 13, 2013, and the subsequent reporting deadlines were in 2015 and 2017. Cambridge Analytica engaged in the illicit collection of Facebook user data from 2014 to 2016, encompassed by the requested reporting period of the assessments.

We will keep both Committees informed of the progress of EPIC's FOIA request for the FTC reports on Facebook compliance. We also urge both Committees to pursue the public release of these documents. They will provide for you a fuller pictures of the FTC's lack of response to the looming privacy crisis in America.

---

[37] Fed. Trade Comm'n., *Statement by the Acting Director of FTC's Bureau of Consumer Protection Regarding Reported Concerns about Facebook Privacy Practices* (March 26, 2018), *https://www.ftc.gov/news-events/press-releases/2018/03/statement-acting-director-ftcs-bureau-consumer-protection. See* EPIC, "FTC Confirms Investigation into Facebook about 2011 Consent Order" (Mar. 26, 2018), *https://epic.org/2018/03/ftc-confirms-investigation-int.html.*

[38] EPIC, "State AGs Launch Facebook Investigation," (Mar. 26, 2018), *https://epic.org/2018/03/state-ags-launch-facebook-inve.html.*

[39] Letter from TACD to Marck Zuckerberg, CEO, Facebook, Inc., Apr. 9, 2018, *http://tacd.org/wp-content/uploads/2018/04/TACD-letter-to-Mark-Zuckerberg_final.pdf.*

[40] Facebook Initial Compliance Report (submitted to FTC on Nov. 13, 2012), *http://epic.org/foia/FTC/facebook/EPIC-13-04-26-FTC-FOIA-20130612-Production-1.pdf;* Facebook Initial Independent Assessment (submitted to FTC on Apr. 22, 2013), *http://epic.org/foia/FTC/facebook/EPIC-14-04-26-FTC-FOIA-20130612-Production-2.pdf.*

Recommendations

There is a lot of work ahead to safeguard the personal data of Americans. Here are a few preliminary recommendations:

- *Improve oversight of the Federal Trade Commission.* The FTC has failed to protect the privacy interests of American consumer and the Commission's inaction contributed directly to the Cambridge Analytica breach, and possibly the Brexit vote and the outcome of the 2016 Presidential election. Oversight of the Commission's failure to enforce the 2011 consent order is critical, particularly for the Senate Commerce Committee which also bears some responsibility for this outcome.
- *Update U.S. privacy laws.* It goes without saying (though obviously it still needs to be said) that U.S. privacy law is out of date. There has always been a gap between changes in technology and business practices and the development of new privacy protections. But the gap today in the United States is the greatest at any time since the emergence of modern privacy law in the 1960s. The current approach is also unnecessarily inefficient, complex, and ineffective. And many of the current proposals, *e.g.,* better privacy notices, would do little to protect privacy or address the problems arising from Cambridge Analytica debacle.
- *Establish a Federal privacy agency in the United States.* The U.S. is one of the few developed countries in the world without a data protection agency. The practical consequence is that the U.S consumers experience the highest levels of data breach, financial fraud, and identity theft in the world. And U.S. businesses, with their vast collections of personal data, remain the target of cyber attack by criminals and foreign adversaries. The longer the U.S. continues on this course, the greater will be the threats to consumer privacy, democratic institutions, and national security.

Conclusion

The transfer of 87 million user records to Cambridge Analytica could have been avoided if the FTC had done its job. The 2011 Consent Order against Facebook was issued to protect the privacy of user data. If it had been enforced, there would be no need for the hearing this week.

After the hearing with Mr. Zuckerberg this week, the Committees should ask current and former FTC Commissioners and key staff, "why didn't you enforce the 2011 Consent Order against Facebook and prevent this mess?"[41]

We ask that this letter be submitted into the hearing record. EPIC looks forward to working with the Committee.

Sincerely,

/s/ MARC ROTENBERG
Marc Rotenberg
EPIC President

/s/ SUNNY KANG
Sunny Kang
EPIC International Consumer Counsel

/s/ CAITRIONA FITZGERALD
Caitriona Fitzgerald
EPIC Policy Director

/s/ SAM LESTER
Sam Lester
EPIC Consumer Privacy Counsel

/s/ ENID ZHOU
Enid Zhou
EPIC Open Government Fellow

Attachment

EPIC, *et al. In the Matter of Facebook, Inc: Complaint, Request for Investigation, Injunction, and Other Relief,* Before the Federal Trade Commission, Washington, DC (Dec. 17, 2009) (29 pages, 119 numbered paragraphs) (signatories include The Electronic Privacy Information Center, The American Library Association, The Center for Digital Democracy, The Consumer Federation of America, Patient Privacy Rights, Privacy Activism, Privacy Rights Now Coalition, The Privacy Rights Clearinghouse, The U.S. Bill of Rights Foundation).

---

[41] *See* Marc Rotenberg, *How the FTC Could Have Prevented the Facebook Mess,* Techonomy (Mar. 22, 2018), *https://techonomy.com/2018/03/how-the-ftc-could-have-avoided-the-facebook-mess/*.

BEFORE THE

FEDERAL TRADE COMMISSION

WASHINGTON, DC

In the Matter of	)
	)
Facebook, Inc.	)
	)
	)

COMPLAINT, REQUEST FOR INVESTIGATION, INJUNCTION, AND OTHER RELIEF

I. Introduction

1. This complaint concerns material changes to privacy settings made by Facebook, the largest social network service in the United States, which adversely impact users of the Facebook service. Facebook's changes to users' privacy settings disclose personal information to the public that was previously restricted. Facebook's changes to users' privacy settings also disclose personal information to third parties that was previously not available. These changes violate user expectations, diminish user privacy, and contradict Facebook's own representations. These business practices are Unfair and Deceptive Trade Practices, subject to review by the Federal Trade Commission (the "Commission") under section 5 of the Federal Trade Commission Act.

2. These business practices impact more than 100 million users of the social networking site who fall within the jurisdiction of the United States Federal Trade Commission.[1]

3. EPIC urges the Commission to investigate Facebook, determine the extent of the harm to consumer privacy and safety, require Facebook to restore privacy settings that were previously available as detailed below, require Facebook to give users meaningful control over personal information, and seek appropriate injunctive and compensatory relief.

II. Parties

4. The Electronic Privacy Information Center ("EPIC") is a not-for-profit research center based in Washington, D.C. EPIC focuses on emerging privacy and civil liberties issues and is a leading consumer advocate before the Federal Trade Commission. Among its other activities, EPIC first brought the Commission's attention to the privacy risks of online advertising.[2] In 2004, EPIC filed a complaint with the FTC regarding the deceptive practices of data broker firm Choicepoint, calling the Commission's attention to "data products circumvent[ing] the FCRA, giving businesses, private investigators, and law enforcement access to data that previously had been subjected to Fair Information Practices."[3] As a result of the EPIC complaint, the FTC fined Choicepoint $15 million.[4] EPIC initiated the complaint to the FTC regarding Microsoft Passport.[5] The Commission subsequently required Microsoft to implement a comprehensive information security program for Passport and similar services.[6] EPIC also filed a complaint with the FTC regarding the marketing

---

[1] Facebook, *Statistics,* http://www.facebook.com/press/info.php?statistics (last visited Dec. 14, 2009); *see also* Eric Eldon, *Facebook Reaches 100 Million Monthly Active Users in the United States,* InsideFacebook.com, Dec. 7, 2009, *http://www.insidefacebook.com/2009/12/07/facebook-reaches-100-million-monthly-active-users-in-the-united-states* (last visited Dec. 15, 2009).

[2] *In the Matter of DoubleClick,* Complaint and Request for Injunction, Request for Investigation and for Other Relief, before the Federal Trade Commission (Feb. 10, 2000), available at *http://epic.org/privacy/internet/ftc/DCLK_complaint.pdf.*

[3] *In the Matter of Choicepoint,* Request for Investigation and for Other Relief, before the Federal Trade Commission (Dec. 16, 2004), available at *http://epic.org/privacy/choicepoint/fcraltr12.16.04.html.*

[4] Federal Trade Commission, *ChoicePoint Settles Data Security Breach Charges; to Pay $10 Million in Civil Penalties,* $5 Million for Consumer Redress, *http://www.ftc.gov/opa/2006/01/choicepoint.shtm* (last visited Dec. 13, 2009).

[5] *In the Matter of Microsoft Corporation,* Complaint and Request for Injunction, Request for Investigation and for Other Relief, before the Federal Trade Commission (July 26, 2001), available at *http://epic.org/privacy/consumer/MS_complaint.pdf.*

[6] *In the Matter of Microsoft Corporation,* File No. 012 3240, Docket No. C–4069 (Aug. 2002), available at *http://www.ftc.gov/os/caselist/0123240/0123240.shtm. See also* Fed. Trade Comm'n, "Microsoft Settles FTC Charges Alleging False Security and Privacy Promises" (Aug. 2002) ("The proposed consent order prohibits any misrepresentation of information practices in connection with Passport and other similar services. It also requires Microsoft to implement and maintain a comprehensive information security program. In addition, Microsoft must have its

of amateur spyware,[7] which resulted in the issuance of a permanent injunction barring sales of CyberSpy's "stalker spyware," over-the-counter surveillance technology sold for individuals to spy on other individuals.[8]

5. Earlier this year, EPIC urged the FTC to undertake an investigation of Google and cloud computing.[9] The FTC agreed to review the complaint, stating that it "raises a number of concerns about the privacy and security of information collected from consumers online."[10] More recently, EPIC asked the FTC to investigate the "parental control" software firm Echometrix.[11] Thus far, the FTC has failed to announce any action in this matter, but once the Department of Defense became aware of the privacy and security risks to military families, it removed Echometrix's software from the Army and Air Force Exchange Service, the online shopping portal for military families.[12]

6. The American Library Association is the oldest and largest library association in the world, with more than 64,000 members. Its mission is "to provide leadership for the development, promotion, and improvement of library and information services and the profession of librarianship in order to enhance learning and ensure access to information for all."

7. The Center for Digital Democracy ("CDD") is one of the leading non-profit groups analyzing and addressing the impact of digital marketing on privacy and consumer welfare. Based in Washington, D.C., CDD has played a key role promoting policy safeguards for interactive marketing and data collection, including at the FTC and Congress.

8. Consumer Federation of America ("CFA") is an association of some 300 nonprofit consumer organizations across the U.S. CFA was created in 1968 to advance the consumer interest through research, advocacy, and education.

9. Patient Privacy Rights is a non-profit organization located in Austin, Texas. Founded in 2004 by Dr. Deborah Peel, Patient Privacy Rights is dedicated to ensuring Americans control all access to their health records.

10. Privacy Activism is a nonprofit organization whose goal is to enable people to make well-informed decisions about the importance of privacy on both a personal and societal level. A key goal of the organization is to inform the public about the importance of privacy rights and the short-and long-term consequences of losing them, either inadvertently, or by explicitly trading them away for perceived or ill-understood notions of security and convenience.

11. The Privacy Rights Clearinghouse ("PRC") is a nonprofit consumer organization with a two-part mission—consumer information and consumer advocacy. It was established in 1992 and is based in San Diego, CA. Among its several goals, PRC works to raise consumers' awareness of how technology affects personal privacy and to empower consumers to take action to control their own personal information by providing practical tips on privacy protection.

12. The U.S. Bill of Rights Foundation is a non-partisan public interest law policy development and advocacy organization seeking remedies at law and public policy improvements on targeted issues that contravene the Bill of Rights and related Constitutional law. The Foundation implements strategies to combat violations of individual rights and civil liberties through Congressional and legal liaisons, coalition building, message development, project planning & preparation, tactical integration with supporting entities, and the filings of complaints and of *amicus curiae* briefs in litigated matters.

13. Facebook Inc. was founded in 2004 and is based in Palo Alto, California. Facebook's headquarters are located at 156 University Avenue, Suite 300, Palo Alto,

---

security program certified as meeting or exceeding the standards in the consent order by an independent professional every two years."), available at *http://www.ftc.gov/opa/2002/08/microst.shtm.*

[7] *In the Matter of Awarenesstech.com, et al.,* Complaint and Request for Injunction, Request for Investigation and for Other relief, before the Federal Trade Commission, available at *http://epic.org/privacy/dv/spy_software.pdf.*

[8] FTC v. Cyberspy Software, No. 6:08-cv-1872 (D. Fla. Nov. 6, 2008) (unpublished order), available at *http://ftc.gov/os/caselist/0823160/081106cyberspytro.pdf.*

[9] *In the Matter of Google, Inc., and Cloud Computing Services,* Request for Investigation and for Other Relief, before the Federal Trade Commission (Mar. 17, 2009), available at *http://epic.org/privacy/cloudcomputing/google/ftc031709.pdf.*

[10] Letter from Eileen Harrington, Acting Director of the FTC Bureau of Consumer Protection, to EPIC (Mar. 18, 2009), available at *http://epic.org/privacy/cloudcomputing/google/031809_ftc_ltr.pdf.*

[11] *In the Matter of Echometrix, Inc.,* Request for Investigation and for Other Relief, before the Federal Trade Commission (Sep. 25, 2009), available at *http://epic.org/privacy/ftc/Echometrix%20FTC%20Complaint%20final.pdf.*

[12] EPIC, *Excerpts from Echometrix Documents, http://epic.org/privacy/echometrix/Excerpts_from_echometrix_docs_12-1-09.pdf* (last visited Dec. 13, 2009).

CA 94301. At all times material to this complaint, Facebook's course of business, including the acts and practices alleged herein, has been and is in or affecting commerce, as "commerce" is defined in Section 4 of the Federal Trade Commission Act, 15 U.S.C. § 45.

III. The Importance of Privacy Protection

14. The right of privacy is a personal and fundamental right in the United States.[13] The privacy of an individual is directly implicated by the collection, use, and dissemination of personal information. The opportunities to secure employment, insurance, and credit, to obtain medical services and the rights of due process may be jeopardized by the misuse of personal information.[14]

15. The excessive collection of personal data in the United States coupled with inadequate legal and technological protections have led to a dramatic increase in the crime of identity theft.[15]

16. The Federal Government has established policies for privacy and data collection on Federal websites that acknowledge particular privacy concerns "when uses of web technology can track the activities of users over time and across different websites" and has discouraged the use of such techniques by Federal agencies.[16]

17. As the Supreme Court has made clear, and the Court of Appeals for the District of Columbia Circuit has recently held, "both the common law and the literal understanding of privacy encompass the individual's control of information concerning his or her person." [17]

18. The Organization for Economic Co-operation and Development ("OECD") Guidelines on the Protection of Privacy and Transborder Flows of Personal Data recognize that "the right of individuals to access and challenge personal data is generally regarded as perhaps the most important privacy protection safeguard."

19. The appropriation tort recognizes the right of each person to protect the commercial value of that person's name and likeness. The tort is recognized in virtually every state in the United States.

20. The Madrid Privacy Declaration of November 2009 affirms that privacy is a basic human right, notes that "corporations are acquiring vast amounts of personal data without independent oversight," and highlights the critical role played by "Fair Information Practices that place obligations on those who collect and process personal information and gives rights to those whose personal information is collected." [18]

21. The Federal Trade Commission is "empowered and directed" to investigate and prosecute violations of Section 5 of the Federal Trade Commission Act where the privacy interests of Internet users are at issue.[19]

IV. Factual Background

Facebook's Size and Reach Is Unparalleled Among Social Networking Sites

22. Facebook is the largest social network service provider in the United States. According to Facebook, there are more than 350 million active users, with more than 100 million in the United States. More than 35 million users update their statuses at least once each day.[20]

---

[13] *See Department of Justice v. Reporters Committee for Freedom of the Press,* 489 U.S. 749, 763 (1989) ("both the common law and the literal understandings of privacy encompass the individual's control of information concerning his or her person"); *Whalen v. Roe,* 429 U.S. 589, 605 (1977); *United States v. Katz,* 389 U.S. 347 (1967); *Olmstead v. United States,* 277 U.S. 438, 478 (1928) (Brandeis, J., dissenting).

[14] Fed. Trade Comm'n, *Consumer Sentinel Network Data Book* 11 (2009) (charts describing how identity theft victims' information have been misused).

[15] *Id.* at 5 (from 2000–2009, the number of identity theft complaints received increased from 31,140 to 313,982); *see* U.S. Gen. Accounting Office, *Identity Theft: Governments Have Acted to Protect Personally Identifiable Information, but Vulnerabilities Remain* 8 (2009); Fed. Trade Comm'n, *Security in Numbers: SSNs and ID Theft* 2 (2008).

[16] Office of Management and Budget, *Memorandum for the Heads of Executive Departments and Agencies* (2000), available at *http://www.whitehouse.gov/omb/memoranda_m00-13* (last visited Dec. 17, 2009).

[17] *U.S. Dep't of Justice v. Reporters Comm. for Freedom of the Press,* 489 U.S. 749, 763 (1989), cited in *Nat'l Cable & Tele. Assn. v. Fed. Commc'ns. Comm'n,* No. 07–1312 (D.C. Cir. Feb. 13, 2009).

[18] The Madrid Privacy Declaration: Global Privacy Standards for a Global World, Nov. 3, 2009, available at *http://thepublicvoice.org/madrid-declaration/*.

[19] 15 U.S.C. § 45 (2006).

[20] Facebook, *Statistics, http://www.facebook.com/press/info.php?statistics* (last visited Dec. 14, 2009).

23. More than 2.5 billion photos are uploaded to the site each month.[21] Facebook is the largest photo-sharing site on the internet, by a wide margin.[22]

24. As of August 2009, Facebook is the fourth most-visited website in the world, and the sixth most-visited website in the United States.[23]

Facebook Has Previously Changed Its Service in Ways that Harm Users' Privacy

25. In September 2006, Facebook disclosed users' personal information, including details relating to their marital and dating status, without their knowledge or consent through its "News Feed" program.[24] Hundreds of thousands of users objected to Facebook's actions.[25] In response, Facebook stated:

> We really messed this one up. When we launched News Feed and Mini-Feed we were trying to provide you with a stream of information about your social world. Instead, we did a bad job of explaining what the new features were and an even worse job of giving you control of them.[26]

26. In 2007, Facebook disclosed users' personal information, including their online purchases and video rentals, without their knowledge or consent through its "Beacon" program.[27]

27. Facebook is a defendant in multiple Federal lawsuits [28] arising from the "Beacon" program.[29] In the lawsuits, users allege violations of Federal and state law, including the Video Privacy Protection Act, the Electronic Communications Privacy Act, the Computer Fraud and Abuse Act, and California's Computer Crime Law.[30]

28. On May 30, 2008, the Canadian Internet Policy and Public Interest Clinic filed a complaint with Privacy Commissioner of Canada concerning the "unnecessary and non-consensual collection and use of personal information by Facebook." [31]

29. On July 16, 2009, the Privacy Commissioner's Office found Facebook "in contravention" of Canada's Personal Information Protection and Electronic Documents Act.[32]

30. The Privacy Commissioner's Office found:

> Facebook did not have adequate safeguards in place to prevent unauthorized access by application developers to users' personal information, and furthermore was not doing enough to ensure that meaningful consent was obtained from individuals for the disclosure of their personal information to application developers.[33]

31. On February 4, 2009, Facebook revised its Terms of Service, asserting broad, permanent, and retroactive rights to users' personal information—even after they

---

[21] *Id.*

[22] Erick Schonfeld, *Facebook Photos Pulls Away From the Pack,* TechCrunch (Feb. 22, 2009), *http://www.techcrunch.com/2009/02/22/facebook-photos-pulls-away-from-the-pack/*.

[23] Erick Schonfeld, *Facebook is Now the Fourth Largest Site in the World,* TechCrunch (Aug. 4, 2009), *http://www.techcrunch.com/2009/08/04/facebook-is-now-the-fourth-largest-site-in-the-world/*.

[24] *See generally* EPIC, *Facebook Privacy, http://epic.org/privacy/facebook/* (last visited Dec. 15, 2009).

[25] Justin Smith, *Scared students protest Facebook's social dashboard, grappling with rules of attention economy,* Inside Facebook (Sept. 6, 2006), *http://www.insidefacebook.com/2006/09/06/scared-students-protest-facebooks-social-dashboard-grappling-with-rules-of-attention-economy/*.

[26] Mark Zuckerberg, *An Open Letter from Mark Zuckerberg* (Sept. 8, 2006), *http://blog.facebook.com/blog.php?post=2208562130.*

[27] *See generally* EPIC, *Facebook Privacy, http://epic.org/privacy/facebook/* (last visited Dec. 15, 2009).

[28] In *Lane v. Facebook, Inc.,* No. 5:08–CV–03845 (N.D. Cal. filed Aug. 12, 2008), Facebook has requested court approval of a class action settlement that would terminate users' claims, but provide no monetary compensation to users. The court has not ruled on the matter.

[29] *See e.g.,* Harris v. Facebook, Inc., No. 09–01912 (N.D. Tex. filed Oct. 9, 2009); *Lane v. Facebook, Inc.,* No. 5:08–CV–03845 (N.D. Cal. filed Aug. 12, 2008); *see also Harris v. Blockbuster,* No. 09–217 (N.D. Tex. filed Feb. 3, 2009), *appeal docketed,* No. 09–10420 (5th Cir. Apr. 29, 2009).

[30] *Id.*

[31] Letter from Philippa Lawson, Director, Canadian Internet Policy and Public Interest Clinic to Jennifer Stoddart, Privacy Commissioner of Canada (May 30, 2008), available at *http://www.cippic.ca/uploads/CIPPICFacebookComplaint_29May08.pdf.*

[32] Elizabeth Denham, Assistant Privacy Commissioner of Canada, *Report of Findings into the Complaint Filed by the Canadian Internet Policy and Public Interest Clinic (CIPPIC) against Facebook Inc. Under the Personal Information Protection and Electronic Documents Act,* July 16, 2009, available at *http://priv.gc.ca/cf-dc/2009/2009_008_0716_e.pdf.*

[33] *Id.* at 3.

deleted their accounts.[34] Facebook stated that it could make public a user's "name, likeness and image for any purpose, including commercial or advertising." [35]

32. Users objected to Facebook's actions, and Facebook reversed the revisions on the eve of an EPIC complaint to the Commission.[36]

Changes in Privacy Settings: "Publicly Available Information"

33. Facebook updated its privacy policy and changed the privacy settings available to users on November 19, 2009 and again on December 9, 2009.[37]

34. Facebook now treats the following categories of personal data as "publicly available information:"

- users' names,
- profile photos,
- lists of friends,
- pages they are fans of,
- gender,
- geographic regions, and
- networks to which they belong.[38]

35. By default, Facebook discloses "publicly available information" to search engines, to Internet users whether or not they use Facebook, and others. According to Facebook, such information can be accessed by "every application and website, including those you have not connected with . . .." [39]

36. Prior to these changes, only the following items were mandatorily "publicly available information:"

- a user's name and
- a user's network.

37. Users also had the option to include additional information in their public search listing. as the screenshot of the original privacy settings for search discovery demonstrates.

---

[34] Chris Walters, *Facebook's New Terms Of Service: "We Can Do Anything We Want With Your Content. Forever."* The Consumerist, Feb. 15, 2009, available at *http://consumerist.com/2009/02/facebooks-new-terms-of-service-we-can-do-anything-we-want-with-your-content-forever.html #reset.*

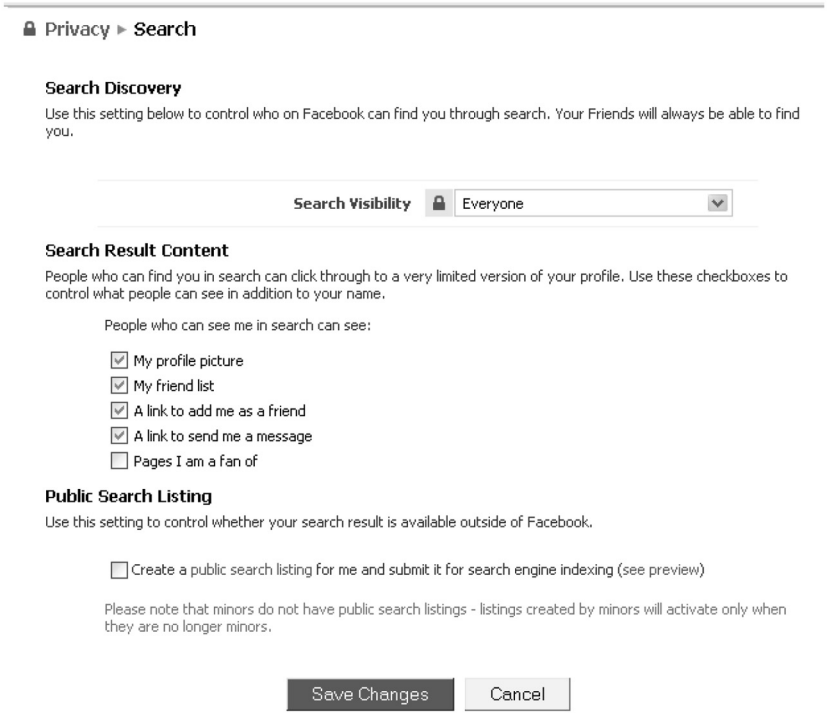
[35] *Id.*

[36] JR Raphael, *Facebook's Privacy Flap: What Really Went Down, and What's Next,* PC World, Feb. 18, 2009, *http://www.pcworld.com/article/159743/facebooks_privacy_flap_what_really_went_down_and_whats_next.html.*

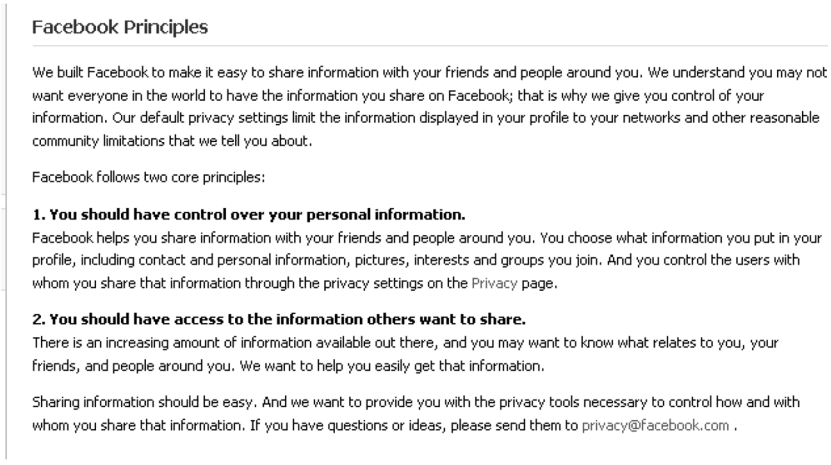
[37] Facebook, *Facebook Asks More Than 350 Million Users Around the World To Personalize Their Privacy* (Dec. 9, 2009), available at *http://www.facebook.com/press/releases.php?p=133917.*

[38] Facebook, *Privacy Policy, http://www.facebook.com/policy.php* (last visited Dec. 16, 2009).

[39] *Id.*



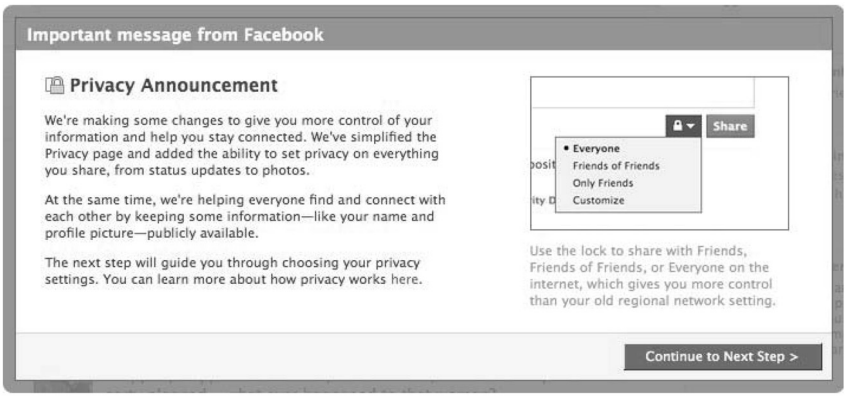
38. Facebook's original privacy policy stated that users "may not want everyone in the world to have the information you share on Facebook" as the screenshot below makes clear:



39. Facebook's Chief Privacy Officer, Chris Kelly, testified before Congress that Facebook gives "users controls over how they share their personal information that model real-world information sharing and provide them transparency about how we

use their information in advertising."[40] Kelly further testified, "many of our users choose to limit what profile information is available to non-friends. Users have extensive and precise controls available to choose who sees what among their networks and friends, as well as tools that give them the *choice* to make a limited set of information available to search engines and other outside entities."[41]

40. In an "Important message from Facebook," Facebook told users it was giving "you more control of your information . . . and [had] added the ability to set privacy on everything you share . . ." as the screen from the transition tool illustrates:



41. Facebook's CEO, Mark Zuckerberg, reversed changes to his personal Facebook privacy settings after the transition from the original privacy settings to the revised settings made public his photographs and other information.[42]

42. Barry Schnitt, Facebook's Director of Corporate Communications and Public Policy, "suggests that users are free to lie about their hometown or take down their profile picture to protect their privacy."[43]

43. Providing false information on a Facebook profile violates Facebook's Terms of Service.[44]

44. Facebook user profile information may include sensitive personal information.

45. Facebook users can indicate that they are "fans" of various organizations, individuals, and products, including controversial political causes.[45]

46. Under the original privacy settings, users controlled public access to the causes they supported. Under the revised settings, Facebook has made users' causes "publicly available information," disclosing this data to others and preventing users from exercising control as they had under the original privacy policy.

47. Based on profile data obtained from Facebook users' friends lists, MIT researchers found that "just by looking at a person's online friends, they could predict whether the person was gay."[46] Under Facebook's original privacy policy, Facebook

---

[40] Testimony of Chris Kelly, Chief Privacy Officer, Facebook, Before the U.S. House or Representatives Committee on Energy and Commerce Subcommittee on Commerce, Trade, and Consumer Protection Subcommittee on Communications, Technology and the Internet (June 18, 2009), available at *http://energycommerce.house.gov/Press_111/20090618/testimony_kelly.pdf.*

[41] *Id.*

[42] Kashmir Hill, *Either Mark Zuckerberg got a whole lot less private or Facebook's CEO doesn't understand the company's new privacy settings* (Dec. 10, 2009), *http://trueslant.com/KashmirHill/2009/12/10/either-mark-zuckerberg-got-a-whole-lot-less-private-or-facebooks-ceo-doesnt-understand-the-companys-new-privacy-settings/.*

[43] Julia Angwin, *How Facebook Is Making Friending Obsolete,* Wall St. J., Dec. 15, 2009, available at *http://online.wsj.com/article/SB126084637203791583.html.*

[44] Facebook, Statement of Rights and Responsibilities, http://www.facebook.com/terms.php (last visited Dec. 16, 2009); *see* Jason Kincaid, *Facebook Suggests You Lie, Break Its Own Terms Of Service To Keep Your Privacy,* Washington Post, Dec. 16, 2009, available at *http://www.washingtonpost.com/wp-dyn/content/article/2009/12/15/AR2009121505270.html.*

[45] *See, e.g.,* Facebook, *Prop 8,* http://www.facebook.com/pages/Prop-8/86610985605 (last visited Dec. 15, 2009); Facebook, *No on Prop 8 Don't Eliminate Marriage for Anyone, http://www.facebook.com/#/pages/No-on-Prop-8-Dont-Eliminate-Marriage-for-Anyone/29097894014* (last visited Dec. 15, 2009); *see also Court Tosses Prop. 8 Ruling on Strategy Papers,* San Francisco Chron. (Dec. 12, 2009), available at *http://www.sfgate.com/cgi-bin/article.cgi?f=/c/a/2009/12/11/BA3A1B34VC.DTL.*

[46] *See* Carolyn Y. Johnson, *Project "Gaydar,"* Sep. 20, 2009, Boston Globe, available at *http://www.boston.com/bostonglobe/ideas/articles/2009/09/20/project_gaydar_an_mit_experiment_raises_new_questions_about_online_privacy/?page=full*

did not categorize users' friends lists as "publicly available information." Facebook now makes users' friends lists "publicly available information."

48. Dozens of American Facebook users, who posted political messages critical of Iran, have reported that Iranian authorities subsequently questioned and detained their relatives.[47] Under the revised privacy settings, Facebook makes such users' friends lists publicly available.

49. According to the Wall Street Journal, one Iranian-American graduate student received a threatening e-mail that read, "we know your home address in Los Angeles," and directed the user to "stop spreading lies about Iran on Facebook."[48]

50. Another U.S. Facebook user who criticized Iran on Facebook stated that security agents in Tehran located and arrested his father as a result of the postings.[49]

51. One Facebook user who traveled to Iran said that security officials asked him whether he owned a Facebook account, and to verify his answer, they performed a Google search for his name, which revealed his Facebook page. His passport was subsequently confiscated for one month, pending interrogation.[50]

52. Many Iranian Facebook users, out of fear for the safety of their family and friends, changed their last name to "Irani" on their pages so government officials would have a more difficult time targeting them and their loved ones.[51]

53. By implementing the revised privacy settings, Facebook discloses users' sensitive friends lists to the public and exposes users to the analysis employed by Iranian officials against political opponents.

Changes to Privacy Settings: Information Disclosure to Application Developers

54. The Facebook Platform transfers Facebook users' personal data to application developers without users' knowledge or consent.[52]

55. Facebook permits third-party applications to access user information at the moment a user visits an application website. According to Facebook, third party applications receive publicly available information automatically when you visit them, and additional information when you formally authorize or connect your Facebook account with them."[53]

56. As Facebook itself explains in its documentation, when a user adds an application, by default that application then gains access to everything on Facebook that the user can see.[54] The primary "privacy setting" that Facebook demonstrates to third-party developers governs what other users can see from the application's output, rather than what data may be accessed by the application.[55]

57. According to Facebook:

> Examples of the types of information that applications and websites may have access to include the following information, to the extent visible on Facebook: your name, your profile picture, your gender, your birthday, your hometown location (city/state/country), your current location (city/state/country), your political view, your activities, your interests, your musical preferences, television shows in which you are interested, movies in which you are interested, books in which you are interested, your favorite quotes, your relationship status, your dating interests, your relationship interests, your network affiliations, your education history, your work history, your course information, copies of photos in your photo albums, metadata associated with your photo albums (*e.g.,* time of upload, album name, comments on your photos, etc.), the total number of messages sent and/or received by you, the total number of unread messages in your in-box, the total number of "pokes" you have sent and/or received, the total number of wall posts on your Wall, a list of user IDs mapped to your friends, your social timeline, notifications that you have received from other applications, and events associated with your profile.[56]

---

[47] Farnaz Fassihi, *Iranian Crackdown Goes Global,* Wall Street Journal (Dec. 4, 2009), available at *http://online.wsj.com/article/SB125978649644673331.html.*

[48] *Id.*

[49] *Id.*

[50] *Id.*

[51] *Id.*

[52] *See* Facebook, *Facebook Platform, http://www.facebook.com/facebook#/platform?v=info* (last visited Dec. 13, 2009).

[53] Facebook, *Privacy Policy, http://www.facebook.com/policy.php* (last visited Dec. 16, 2009).

[54] Facebook, *About Platform, http://developers.facebook.com/about_platform.php* (last visited Dec. 16, 2009).

[55] Facebook Developer Wiki, *Anatomy of a Facebook App, http://wiki.developers.facebook.com/index.php/Anatomy_of_a_Facebook_App#Privacy_Settings* (last visited Dec. 16, 2009).

[56] Facebook, *About Platform, http://developers.facebook.com/about_platform.php* (last visited Dec. 16, 2009).

58. To access this information, developers use the Facebook Application Programming Interface ("API"), to "utiliz[e] profile, friend, Page, group, photo, and event data."[57] The API is a collection of commands that an application can run on Facebook, including authorization commands, data retrieval commands, and data publishing commands.[58]

59. Third-parties who develop Facebook applications may also transmit the user information they access to their own servers, and are asked only to retain the information for less than 24 hours.[59]

60. A 2007 University of Virginia study of Facebook applications found that "90.7 percent of applications are being given more privileges than they need."[60]

61. According to the Washington Post, many Facebook developers who have gained access to information this way have considered the "value" of having the data, even when the data is not relevant to the purpose for which the user has added the application.[61]

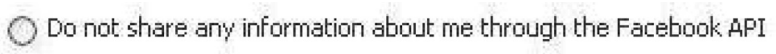
62. Under the revised privacy policy, Facebook now categorizes users' names, profile photos, lists of friends, pages they are fans of, gender, geographic regions, and networks to which they belong as "publicly available information," and Facebooks sets the "default privacy setting for certain types of information [users] post on Facebook . . . to 'everyone.'"[62]

63. Facebook allows user information that is categorized as publicly available to "everyone" to be: "accessed by everyone on the Internet (including people not logged into Facebook);" made subject to "indexing by third party search engines;" "associated with you outside of Facebook (such as when you visit other sites on the internet);" and "imported and exported by us and others *without* privacy limitations."[63]

64. With the Preferred Developer Program, Facebook will give third-party developers access to a user's primary e-mail address, personal information provided by the user to Facebook to subscribe to the Facebook service, but not necessarily available to the public or to developers.[64] In fact, some users may choose to create a Facebook account precisely to prevent the disclosure of their primary e-mail address.

65. Facebook states in the revised privacy policy that users can "opt-out of Facebook Platform and Facebook Connect altogether through [their] privacy settings."[65] Facebook further states that, "you can control how you share information with those third-party applications and websites through your application settings."[66]

66. In fact, under the original privacy settings, users had a one-click option to prevent the disclosure of personal information to third party application developers through the Facebook API, as the screenshot below indicates:



67. Under the revised privacy settings, Facebook has eliminated the universal one-click option and replaced it with the screen illustrated below:[67]

---

[57] Facebook Developer Wiki, *API, http://wiki.developers.facebook.com/index.php/API* (last visited Dec. 16, 2009).

[58] *Id.*

[59] Facebook Developer Wiki, *Policy Examples and Explanations/Data and Privacy, http://wiki.developers.facebook.com/index.php/Policy_Examples_and_Explanations/Data_and_Privacy* (last visited Dec. 16, 2009).

[60] Adrienne Felt & David Evans, *Privacy Protection for Social Networking APIs, http://www.cs.virginia.edu/felt/privacy/* (last visited Dec. 16, 2009).

[61] Kim Hart, *A Flashy Facebook Page, at a Cost to Privacy,* Wash. Post, June 12, 2008, available at *http://www.washingtonpost.com/wp-dyn/content/article/2008/06/11/AR2008061103759.html*

[62] Facebook, *Privacy Policy, http://www.facebook.com/policy.php* (last visited Dec. 16, 2009).

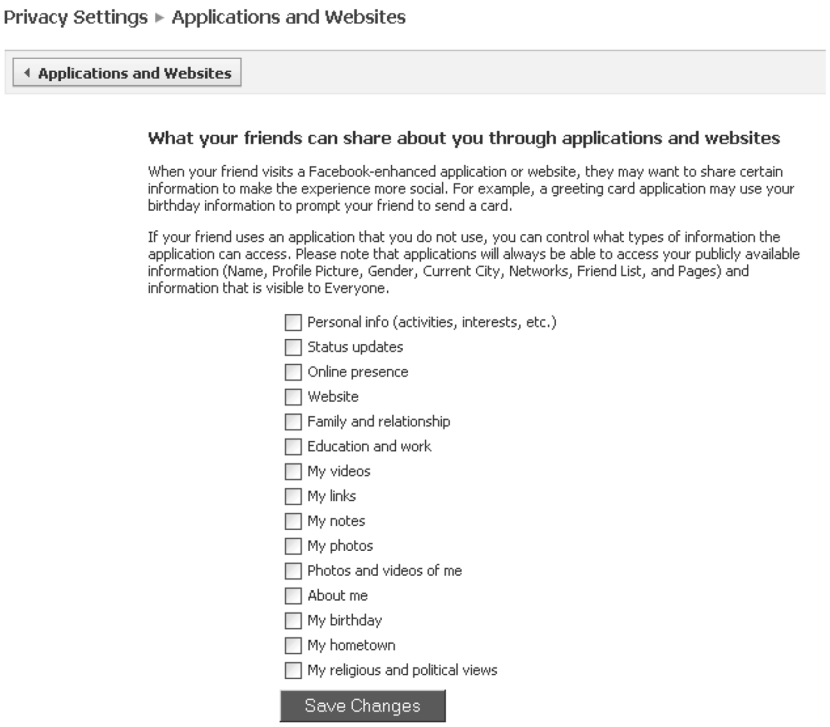
[63] *Id.* (emphasis added)

[64] Facebook, *Developer Roadmap, http://wiki.developers.facebook.com/index.php/Developer_Roadmap* (last visited Dec. 17 2009); Facebook, *Roadmap E-mail, http://wiki.developers.facebook.com/index.php/Roadmap_E-mail* (last visited Dec. 17, 2009); *see also* Mark Walsh, *Facebook Starts Preferred Developer Program* (Dec. 17, 2009), *http://www.mediapost.com/publications/?fa=Articles.showArticle&art_aid=119293.*

[65] Facebook, *Privacy Policy, http://www.facebook.com/policy.php* (last visited Dec. 16, 2009).

[66] *Id.*

[67] Facebook, *Privacy Settings, http://www.facebook.com/settings/?tab=privacy&section=applications&field=friends_share* (last visited Dec. 13, 2009).



68. Under the revised settings, even when a user unchecks all boxes and indicates that none of the personal information listed above should be disclosed to third party application developers, Facebook states that "applications will *always* be able to access your publicly available information (Name, Profile Picture, Gender, Current City, Networks, Friend List, and Pages) and information that is visible to Everyone." [68]

69. Facebook's "Everyone" setting overrides the user's choice to limit access by third-party applications and websites.

70. Facebook does not now provide the option that explicitly allows users to opt out of disclosing all information to third parties through the Facebook Platform.

71. Users can block individual third-party applications from obtaining personal information by searching the Application Directory, visiting the application's "about" page, clicking a small link on that page, and then confirming their decision.[69] A user would have to perform these steps for each of more than 350,000 applications in order to block all of them.[70]

Facebook Users Oppose the Changes to the Privacy Settings

72. Facebook users oppose these changes. In only four days, the number of Facebook groups related to privacy settings grew to more than five hundred.[71] Many security experts, bloggers, consumer groups, and news organizations have also opposed these changes.

73. More than 1,050 Facebook users are members of a group entitled "Against The New Facebook Privacy Settings!" The group has a simple request: "We demand that

---

[68] *Id.* (emphasis added)

[69] Facebook, *General Application Support: Application Safety and Security, http://www.facebook.com/help.php?page=967* (last visited Dec. 14, 2009).

[70] Facebook, *Statistics, http://www.facebook.com/press/info.php?statistics* (last visited Dec. 14, 2009).

[71] Facebook, *Search "privacy settings," http://www.facebook.com/search/?o=69&init=s%3Agroup&q=privacy%20settings* (last visited Dec. 15, 2009).

Facebook stop forcing people to reveal things they don't feel comfortable revealing." [72]

74. More than 950 Facebook users are members of a group entitled "Facebook! Fix the Privacy Settings," which exhorts users to "tell Facebook that our personal information is private, and we want to control it!" [73]

75. More than 74,000 Facebook users are members of a group entitled "Petition: Facebook, stop invading my privacy!" [74] The group objects to the revisions and hopes to "get a message across to Facebook." [75] The group description explains, "[o]n December 9, 2009 Facebook once again breached our privacy by imposing new 'privacy settings' on 365+ million users. These settings notably give us LESS privacy than we had before, so I ask, how exactly do they make us more secure?. . . . Perhaps the most frustrating and troublesome part is the changes Facebook made on our behalf without truly making us aware or even asking us." [76]

76. A Facebook blog post discussing the changes to Facebook's privacy policy and settings drew 2,000 comments from users, most of them critical of the changes.[77] One commenter noted, "I came here to communicate with people with whom I have some direct personal connection; not to have my personal information provided to unscrupulous third party vendors and made available to potential stalkers and identity thieves." [78] Another commented, "I liked the old privacy settings better. I felt safer and felt like I had more control." [79]

77. The Electronic Frontier Foundation posted commentary online discussing the "good, the bad, and the ugly" aspects of Facebook's revised privacy policy and settings. More than 400 people have "tweeted" this article to encourage Facebook users to read EFF's analysis.[80]

78. The American Civil Liberties Union of Northern California's Demand Your dotRights campaign started a petition to Facebook demanding that Facebook (1) give full control of user information back to users; (2) give users strong default privacy settings; and (3) restrict the access of third party applications to user data.[81] The ACLU is "concerned that the changes Facebook has made actually remove some privacy controls and encourage Facebook users to make other privacy protections disappear." [82]

79. In the past week, more than 3,000 blog posts have been written focusing on criticism of Facebook's privacy changes.[83]

80. After rolling out the revised Facebook privacy settings, widespread user criticism of the change in the "view friends" setting prompted Facebook to roll back the changes in part: "In response to your feedback, we've improved the Friend List visibility option described below. Now when you uncheck the 'Show my friends on my profile' option in the Friends box on your profile, your Friend List won't appear on your profile regardless of whether people are viewing it while logged into Facebook or logged out." Facebook further stated that "this information is still publicly available, however, and can be accessed by applications." [84]

81. Ed Felten, a security expert and Princeton University professor,[85] stated:

---

[72] Facebook, *Against The New Facebook Privacy Settings!, http://www.facebook.com/group.php?gid=209833062912* (last visited Dec. 15, 2009).

[73] Facebook, *Facebook! Fix the Privacy Settings, http://www.facebook.com/group.php?gid=192282128398* (last visited Dec. 15, 2009).

[74] Facebook, *Petition: Facebook, stop invading my privacy!, http://www.facebook.com/group.php?gid=5930262681&ref=share* (last visited Dec. 15, 2009).

[75] *Id.*

[76] *Id.*

[77] *See* The Facebook Blog, *Updates on Your New Privacy Tools, http://blog.facebook.com/blog.php?post=197943902130* (last visited Dec. 14, 2009).

[78] *Id.*

[79] *Id.*

[80] *See* Twitter, *Twitter Search "eff.org Facebook," http://twitter.com/#search?q=eff.org%20facebook* (last visited Dec. 14, 2009).

[81] American Civil Liberties Union, *Demand Your dotRights: Facebook Petition, https://secure.aclu.org/site/SPageNavigator/CN_Facebook_Privacy_Petition* (last visited Dec. 15, 2009).

[82] *Id; see also* ACLUNC dotRights, *What Does Facebook's Privacy Transition Mean for You?, http://dotrights.org/what-does-facebooks-privacy-transition-mean-you* (last visited Dec. 16, 2009).

[83] *See* Google, *Google Blog Search "facebook privacy criticism," http://blogsearch.google.com/blogsearch?client=news&hl=en&q=facebook+privacy+criticism&ie=UTF-8&as_drrb=q&as_qdr=w* (last visited Dec. 14, 2009).

[84] The Facebook Blog, *Updates on Your New Privacy Tools, http://blog.facebook.com/blog.php?post=197943902130* (last visited Dec. 14, 2009).

[85] Prof. Felton is also Director of the Princeton Center for Information Technology Policy, a cross-disciplinary effort studying digital technologies in public life.

> As a user myself, I was pretty unhappy about the recently changed privacy control. I felt that Facebook was trying to trick me into loosening controls on my information. Though the initial letter from Facebook founder Mark Zuckerberg painted the changes as pro-privacy. . .the actual effect of the company's suggested new policy was to allow more public access to information. Though the company has backtracked on some of the changes, problems remain.[86]

82. Joseph Bonneau, a security expert and University of Cambridge researcher, criticized Facebook's disclosure of users' friend lists, observing,

> there have been many research papers, including a few by me and colleagues in Cambridge, concluding that [friend lists are] actually the most important information to keep private. The threats here are more fundamental and dangerous-unexpected inference of sensitive information, cross-network deanonymisation, socially targeted phishing and scams.[87]

Bonneau predicts that Facebook "will likely be completely crawled fairly soon by professional data aggregators, and probably by enterprising researchers soon after."[88]

83. Security expert[89] Graham Cluley stated:

> if you make your information available to "everyone," it actually means "everyone, forever." Because even if you change your mind, it's too late—and although Facebook say they will remove it from your profile they will have no control about how it is used outside of Facebook.

Cluley further states, "there's a real danger that people will go along with Facebook's recommendations without considering carefully the possible consequences."[90]

84. Other industry experts anticipated the problems that would result from the changes in Facebook's privacy settings. In early July, TechCrunch, Jason Kincaid wrote:

> Facebook clearly wants its users to become more comfortable sharing their content across the web, because that's what needs to happen if the site is going to take Twitter head-on with real-time search capabilities Unfortunately that's far easier said than done for the social network, which has for years trumpeted its granular privacy settings as one of its greatest assets.[91]

Kincaid observed that "Facebook sees its redesigned control panel as an opportunity to invite users to start shrugging off their privacy. So it's piggybacking the new 'Everyone' feature on top of the Transition Tool . . ."[92]

85. Following the changes in Facebook privacy settings, noted blogger Danny Sullivan wrote, "I came close to killing my Facebook account this week." He went on to say, "I was disturbed to discover things I previously had as options were no longer in my control." Sullivan, the editor of Search Engine Land and an expert in search engine design,[93] concluded:

> I don't have time for this. I don't have time to try and figure out the myriad of ways that Facebook may or may not want to use my information. That's why I almost shut down my entire account this week. It would be a hell of a lot easier than this mess.[94]

---

[86] Ed Felten, *Another Privacy Misstep from Facebook* (Dec. 14, 2009), *http://www.freedom-to-tinker.com/blog/felten/another-privacy-misstep-facebook.*

[87] Joseph Bonneau, *Facebook Tosses Graph Privacy into the Bin* (Dec. 11, 2009), *http://www.lightbluetouchpaper.org/2009/12/11/facebook-tosses-graph-privacy-into-the-bin/; see also* Arvind Narayanan and Vitaly Shmatikov, *De-Anonymizing Social Networks,* available at *http://www.scribd.com/doc/15021482/DeAnonymizing-Social-Networks-Shmatikov-Narayanan; Phishing Attacks Using Social Networks, http://www.indiana.edu/~phishing/social-network-experiment/* (last visited Dec. 15, 2009).

[88] Bonneau, *Facebook Tosses Graph Privacy into the Bin.*

[89] Wikipedia, *Graham Cluley, http://en.wikipedia.org/wiki/Graham_Cluley.*

[90] Graham Cluley, *Facebook privacy settings: What you need to know* (Dec. 10, 2009) *http://www.sophos.com/blogs/gc/g/2009/12/10/facebook-privacy/.*

[91] Jason Kincaid, *The Looming Facebook Privacy Fiasco* (July 1, 2009), *http://www.techcrunch.com/2009/07/01/the-looming-facebook-privacy-fiasco/.*

[92] *Id.*

[93] Wikipedia, *Danny Sullivan (technologist), http://en.wikipedia.org/wiki/Danny_Sullivan_(technologist)* (last visited Dec. 15, 2009).

[94] Danny Sullivan, *Now Is It Facebook's Microsoft Moment?* (Dec. 11, 2009), *http://daggle.com/facebooks-microsoft-moment-1556.*

86. Carleton College librarian Iris Jastram states that the privacy trade-off resulting from the Facebook changes is not "worth it." She writes,

> I'm already making concessions by making myself available to the students who want to friend me there and by grudgingly admitting that I like the rolodex function it plays. But I feel zero motivation to give up more than I can help to Facebook and its third party developers. They can kindly leave me alone, please.[95]

87. Chris Bourg, manager of the Information Center at Stanford University Libraries, notes that "[t]here are some concerns with the new default/recommended privacy settings, which make your updates visible to Everyone, including search engines."[96]

88. Reuters columnist Felix Salmon learned of Facebook's revised privacy settings when Facebook disclosed his "friends" list to critics, who republished the personal information. Salmon apologized to his friends and denounced the Facebook "Everyone" setting:

> I'm a semi-public figure, and although I might not be happy with this kind of cyberstalking, I know I've put myself out there and that there will be consequences of that. But that decision of mine shouldn't have some kind of transitive property which feeds through to my personal friends, and I don't want the list of their names to be publicly available to everyone.[97]

89. In a blog post responding to the revisions, Marshall Kirkpatrick of ReadWriteWeb wrote, "the company says the move is all about helping users protect their privacy and connect with other people, but the new default option is to change from 'old settings' to becoming visible to 'everyone.' . . . This is not what Facebook users signed up for. It's not about privacy at all, it's about increasing traffic and the visibility of activity on the site."[98]

90. Jared Newman of PC World details Facebook's privacy revisions.[99] He is particularly critical of the "Everyone" setting:

> By default, Facebook suggests sharing everything on your profile to make it 'easier for friends to find, identify and learn about you.' It should read, 'make it easier for anyone in the world to find, identify and learn about you.' A little creepier, sure, but this is part of Facebook's never-ending struggle to be, essentially, more like Twitter. Thing is, a lot of people like Facebook because it isn't like Twitter. Don't mess with a good thing.[100]

91. Rob Pegoraro blogged on the Washington Post's "Faster Forward" that the Facebook changes were "more of a mess than I'd expected." He criticized the revised "Everyone" privacy setting, stating the change "should never have happened. *Both from a usability and a PR perspective, the correct move would have been to leave users' settings as they were, especially for those who had already switched their options from the older defaults.*"[101]

92. In another Washington Post story, Cecilia Kang warned users, "post with care."[102] According to Kang:

> While Facebook users will be able to choose their privacy settings, the problem is that most people don't take the time to do so and may simply stick with the defaults. Others may find the process confusing and may not understand how

---

[95] Iris Jastram, *Dear Facebook: Leave Me Alone,* Pegasus Librarian Blog (Dec. 10, 2009), *http://pegasuslibrarian.com/2009/12/dear-facebook-leave-me-alone.html.*

[96] Chris Bourg, *Overview of new Facebook Privacy Settings,* Feral Librarian (Dec. 9, 2009), *http://chrisbourg.wordpress.com/2009/12/09/overview-of-new-facebook-privacy-settings/.*

[97] Felix Salmon, *Why Can't I Hide My List of Facebook Friends?,* Reuters (Dec. 10, 2009), *http://blogs.reutes.com/felix-salmon/2009/12/10/why-cant-i-hide-my-list-of-facebook-friends/.*

[98] Marshall Kirkpatrick, ReadWriteWeb, *The Day Has Come: Facebook Pushes People to Go Public, http://www.readwriteweb.com/archives/facebook_pushes_people_to_go_public.php* (last visited Dec. 14, 2009).

[99] *http://www.pcworld.com/article/184465/facebook_privacy_changes_the_good_and_the_bad.html*

[100] *Id.*

[101] Rob Pegoraro, *Facebook's new default: Sharing updates with 'Everyone',* Washington Post, Dec. 10, 2009, available at *http://voices.washingtonpost.com/fasterforward/2009/12/facebook_default_no-privacy.html* (emphasis added)

[102] Cecilia Kang, *Facebook adopts new privacy settings to give users more control over content,* Washington Post, Dec. 10, 2009, available at *http://www.washingtonpost.com/wp-dyn/content/article/2009/12/09/AR2009120904200.html?hpid=topnews.*

to adjust those settings. Facebook said about one in five users currently adjusts privacy settings.[103]

93. New York Times technology writer Brad Stone reported that these changes have not been welcomed by many users.[104] One user wrote:

> It's certainly a violation of my privacy policy. My own 'personal' privacy policy specifically states that I will not share information about my friends with any potential weirdos, child molesters, homicidal maniacs, or anyone I generally don't like.[105]

94. Stone invited readers to comment on their understanding of the changes. Of the more than 50 responses received, most expressed confusion, concern, or anger. One user explained,

> I find the changes to be the exact opposite of what Facebook claims them to be. Things that were once private for me, and for carefully selected Facebook friends, are now open to everyone on the Internet. This is simply not what I signed up for. These are not the privacy settings I agreed to. It is a complete violation of privacy, not the other way around.[106]

95. Another Facebook user wrote,

> There are users like myself that joined Facebook because we were able to connect with friends and family while maintaining our privacy and now FB has taken that away. Im [*sic*] wondering where are the millions of users that told FB it would be a good idea to offer real-time search results of their FB content on Google.[107]

96. A Boston Globe editorial, "Facebook's privacy downgrade," observes that "Facebook's subtle nudges toward greater disclosure coincided with other disconcerting changes: The site is treating more information, such as a user's home city and photo, as 'publicly available information' that the user cannot control. Over time, privacy changes can only alienate users." Instead, the Globe argues, "Facebook should be helping its 350 million members keep more of their information private."[108]

97. An editorial from the L.A. Times states simply "what's good for the social networking site isn't necessarily what's good for users."[109]

V. Legal Analysis

The FTC's Section 5 Authority

98. Facebook is engaging in unfair and deceptive acts and practices.[110] Such practices are prohibited by the FTC Act, and the Commission is empowered to enforce the Act's prohibitions.[111] These powers are described in FTC Policy Statements on Deception[112] and Unfairness.[113]

99. A trade practice is unfair if it "causes or is likely to cause substantial injury to consumers which is not reasonably avoidable by consumers themselves and not outweighed by countervailing benefits to consumers or to competition."[114]

---

[103] *Id.*

[104] Brad Stone, *Facebook's Privacy Changes Draw More Scrutiny,* N.Y. Times, Dec. 10, 2009, available at *http://bits.blogs.nytimes.com/2009/12/10/facebooks-privacy-changes-draw-more-scrutiny.*

[105] *Id.*

[106] *Id.*

[107] Riva Richmond, *The New Facebook Privacy Settings: A How-To,* N.Y. Times, Dec. 11, 2009, available at *http://gadgetwise.blogs.nytimes.com/2009/12/11/the-new-facebook-privacy-settings-a-how-to/?em.*

[108] Editorial, *Facebook's privacy downgrade,* Boston Globe, Dec. 16, 2009, available at *http://www.boston.com/bostonglobe/editorial_opinion/editorials/articles/2009/12/16/facebooks_privacy_downgrade.*

[109] Editorial, *The business of Facebook,* L.A. Times, Dec. 12, 2009, available at *http://www.latimes.com/news/opinion/editorials/la-ed-facebook12–2009dec12,0,4419776.story.*

[110] *See* 15 U.S.C. § 45.

[111] *Id.*

[112] Fed. Trade Comm'n, FTC Policy Statement on Deception (1983), *available at http://www.ftc.gov/bcp/policystmt/ad-decept.htm* [*hereinafter* FTC Deception Policy].

[113] Fed. Trade Comm'n, FTC Policy Statement on Unfairness (1980), available at *http://www.ftc.gov/bcp/policystmt/ad-unfair.htm* [*hereinafter* FTC Unfairness Policy].

[114] 15 U.S.C. § 45(n); *see, e.g., Fed. Trade Comm'n v. Seismic Entertainment Productions, Inc.,* Civ. No. 1:04–CV–00377 (Nov. 21, 2006) (finding that unauthorized changes to users' computers

Continued

100. The injury must be "substantial." [115] Typically, this involves monetary harm, but may also include "unwarranted health and safety risks." [116] Emotional harm and other "more subjective types of harm" generally do not make a practice unfair.[117] Secondly, the injury "must not be outweighed by an offsetting consumer or competitive benefit that the sales practice also produces." [118] Thus the FTC will not find a practice unfair "unless it is injurious in its net effects." [119] Finally, "the injury must be one which consumers could not reasonably have avoided." [120] This factor is an effort to ensure that consumer decision making still governs the market by limiting the FTC to act in situations where seller behavior "unreasonably creates or takes advantage of an obstacle to the free exercise of consumer decision-making." [121] Sellers may not withhold from consumers important price or performance information, engage in coercion, or unduly influence highly susceptible classes of consumers.[122]

101. The FTC will also look at "whether the conduct violates public policy as it has been established by statute, common law, industry practice, or otherwise." [123] Public policy is used to "test the validity and strength of the evidence of consumer injury, or, less often, it may be cited for a dispositive legislative or judicial determination that such injury is present." [124]

102. The FTC will make a finding of deception if there has been a "representation, omission or practice that is likely to mislead the consumer acting reasonably in the circumstances, to the consumer's detriment." [125]

103. First, there must be a representation, omission, or practice that is likely to mislead the consumer.[126] The relevant inquiry for this factor is not whether the act or practice actually misled the consumer, but rather whether it is likely to mislead.[127] Second, the act or practice must be considered from the perspective of a reasonable consumer.[128] "The test is whether the consumer's interpretation or reaction is reasonable." [129] The FTC will look at the totality of the act or practice and ask questions such as "how clear is the representation? How conspicuous is any qualifying information? How important is the omitted information? Do other sources for the omitted information exist? How familiar is the public with the product or service?" [130]

104. Finally, the representation, omission, or practice must be material.[131] Essentially, the information must be important to consumers. The relevant question is whether consumers would have chosen another product if the deception had not occurred.[132] Express claims will be presumed material.[133] Materiality is presumed for claims and omissions involving "health, safety, or other areas with which the reasonable consumer would be concerned." [134] The harms of this social networking site's practices are within the scope of the FTC's authority to enforce Section 5 of the FTC Act and its purveyors should face FTC action for these violations.

---

that affected the functionality of the computers as a result of Seismic's anti-spyware software constituted a "substantial injury without countervailing benefits.").

[115] FTC Unfairness Policy, *supra* note 113.

[116] *Id.; see, e.g., Fed. Trade Comm'n v. Information Search, Inc.,* Civ. No. 1:06–cv–01099 (Mar. 9, 2007) ("The invasion of privacy and security resulting from obtaining and selling confidential customer phone records without the consumers' authorization causes substantial harm to consumers and the public, including, but not limited to, endangering the health and safety of consumers.").

[117] FTC Unfairness Policy, *supra* note 113.

[118] *Id.*

[119] *Id.*

[120] *Id.*

[121] *Id.*

[122] *Id.*

[123] *Id.*

[124] *Id.*

[125] FTC Deception Policy, *supra* note 112.

[126] FTC Deception Policy, *supra* note 112; *see, e.g., Fed Trade Comm'n v. Pantron I Corp.,* 33 F.3d 1088 (9th Cir. 1994) (holding that Pantron's representation to consumers that a product was effective at reducing hair loss was materially misleading, because according to studies, the success of the product could only be attributed to a placebo effect, rather than on scientific grounds).

[127] FTC Deception Policy, *supra* note 112.

[128] *Id.*

[129] *Id.*

[130] *Id.*

[131] *Id.*

[132] *Id.*

[133] *Id.*

[134] *Id.*

Material Changes to Privacy Practices and Misrepresentations of Privacy Policies Constitute Consumer Harm

105. Facebook's actions injure users throughout the United States by invading their privacy; allowing for disclosure and use of information in ways and for purposes other than those consented to or relied upon by such users; causing them to believe falsely that they have full control over the use of their information; and undermining the ability of users to avail themselves of the privacy protections promised by the company.

106. The FTC Act empowers and directs the FTC to investigate business practices, including data collection practices, that constitute consumer harm.[135] The Commission realizes the importance of transparency and clarity in privacy policies. "Without real transparency, consumers cannot make informed decisions about how to share their information."[136]

107. The FTC recently found that Sears Holding Management Corporations business practices violated the privacy of its customers.[137] The consent order arose from the company's use of software to collect and disclose users' online activity to third parties, and a misleading privacy policy that did not "adequately [inform consumers as to] the full extent of the information the software tracked."[138] The order requires that the company fully, clearly, and prominently disclose the "types of data the software will monitor, record, or transmit."[139] Further, the company must disclose to consumers whether and how this information will be used by third parties.[140]

108. The Commission has also obtained a consent order against an online company for changing its privacy policy in an unfair and deceptive manner. In 2004, the FTC charged Gateway Learning Corporation with making a material change to its privacy policy, allowing the company to share users' information with third parties, without first obtaining users' consent.[141] This was the first enforcement action to "challenge deceptive and unfair practices in connection with a company's material change to its privacy policy."[142] Gateway Learning made representations on the site's privacy policy, stating that consumer information would not be sold, rented or loaned to third parties.[143] In violation of these terms, the company began renting personal information provided by consumers, including gender, age and name, to third parties.[144] Gateway then revised its privacy policy to provide for the renting of consumer information "from time to time," applying the policy retroactively.[145] The settlement bars Gateway Learning from, among other things, "misrepresent[ing] in any manner, expressly or by implication . . . the manner in which Respondent will collect, use, or disclose personal information."[146]

109. Furthermore, the FTC has barred deceptive claims about privacy and security policies with respect to personally identifiable, or sensitive, information.[147] In 2008, the FTC issued an order prohibiting Life is Good, Inc. from "misrepresent[ing] in any manner, expressly or by implication, the extent to which respondents maintain and protect the privacy, confidentiality, or integrity of any personal information collected from or about consumers."[148] The company had represented to its customers, "we are committed to maintaining our customers' privacy," when in fact, it did not have secure or adequate measures of protecting personal information.[149] The

---

[135] 15 U.S.C. § 45.

[136] Remarks of David C. Vladeck, Director, FTC Bureau of Consumer Protection, New York University: "Promoting Consumer Privacy: Accountability and Transparency in the Modern World" (Oct. 2, 2009).

[137] In re Sears Holdings Mgmt. Corp., No. C–4264 (2009) (decision and order), available at *http://www.ftc.gov/os/caselist/0823099/090604searsdo.pdf.*

[138] In re Sears Holdings Mgmt. Corp., No. C–4264 (2009) (complaint), available at *http://www.ftc.gov/os/caselist/0823099/090604searscmpt.pdf* (last visited Sep. 25, 2009).

[139] In re Sears Holdings Mgmt. Corp., No. C–4264 (2009) (decision and order), available at *http://www.ftc.gov/os/caselist/0823099/090604searsdo.pdf.*

[140] *Id.*

[141] Press Release, FTC, Gateway Learning Settles FTC Privacy Charges (July 7, 2004), *http://www.ftc.gov/opa/2004/07/gateway.shtm.*

[142] *Id.*

[143] In re Gateway Learning Corp., No. C–4120 (2004) (complaint), available at *http://www.ftc.gov/os/caselist/0423047/040917comp0423047.pdf.*

[144] *Id.*

[145] *Id.*

[146] In re Gateway Learning Corp., No. C–4120 (2004) (decision and order), available at *http://www.ftc.gov/os/caselist/0423047/040917do0423047.pdf.*

[147] In re Life is Good, No. C–4218 (2008) (decision and order), available at *http://www.ftc.gov/os/caselist/0723046/080418do.pdf.*

[148] *Id.*

[149] *Id.*

Commission further ordered the company to establish comprehensive privacy protection measures in relation to its customers' sensitive information.[150]

Facebook's Revisions to the Privacy Settings Constitute an Unfair and Deceptive Trade Practice

110. Facebook represented that users "may not want everyone in the world to have the information you share on Facebook," and that users "have extensive and precise controls available to choose who sees what among their network and friends, as well as tools that give them the *choice* to make a limited set of information available to search engines and other outside entities." [151]

111. Facebook's changes to users' privacy settings and associated policies in fact categorize as "publicly available information" users' names, profile photos, lists of friends, pages they are fans of, gender, geographic regions, and networks to which they belong.[152] Those categories of user data are no longer subject to users' privacy settings.

112. Facebook represented that its changes to its policy settings and associated policies regarding application developers permit users to "opt-out of Facebook Platform and Facebook Connect altogether through [their] privacy settings," [153] and tells users, "you can control how you share information with those third-party applications and websites through your application settings" [154]

113. Facebook's changes to users' privacy settings and associated policies regarding application developers in fact eliminate the universal one-click option for opting out of Facebook Platform and Facebook Connect, and replaces it with a less comprehensive option that requires users to provide application developers with personal information that users could previously prevent application developers from accessing.[155]

114. Facebook's representations regarding its changes to users' privacy settings and associated policies are misleading and fail to provide users clear and necessary privacy protections.

115. Wide opposition by users, commentators, and advocates to the changes to Facebook's privacy settings and associated policies illustrate that the changes injure Facebook users and harm the public interest.

116. Absent injunctive relief by the Commission, Facebook is likely to continue its unfair and deceptive business practices and harm the public interest.

117. Absent injunctive relief by the Commission, the privacy safeguards for consumers engaging in online commerce and new social network services will be significantly diminished.

VI. Prayer for Investigation and Relief

118. EPIC requests that the Commission investigate Facebook, enjoin its unfair and deceptive business practices, and require Facebook to protect the privacy of Facebook users. Specifically, EPIC requests the Commission to:

> Compel Facebook to restore its previous privacy settings allowing users to choose whether to publicly disclose personal information, including name, current city, and friends;
>
> Compel Facebook to restore its previous privacy setting allowing users to fully opt out of revealing information to third-party developers;
>
> Compel Facebook to make its data collection practices clearer and more comprehensible and to give Facebook users meaningful control over personal information provided by Facebook to advertisers and developers; and
>
> Provide such other relief as the Commission finds necessary and appropriate.

---

[150] *Id.*

[151] Testimony of Chris Kelly, Chief Privacy Officer, Facebook, Before the U.S. House or Representatives Committee on Energy and Commerce Subcommittee on Commerce, Trade, and Consumer Protection Subcommittee on Communications, Technology and the Internet (June 18, 2009), available at *http://energycommerce.house.gov/Press_111/20090618/testimony_kelly.pdf.*

[152] Facebook, *Privacy Policy, http://www.facebook.com/policy.php* (last visited Dec. 13, 2009).

[153] *Id.*

[154] *Id.*

[155] Facebook, *Privacy Settings, http://www.facebook.com/settings/?tab=privacy&section=applications&field=friends_share* (last visited Dec. 13, 2009).

119. EPIC reserves the right to supplement this petition as other information relevant to this proceeding becomes available.

Respectfully Submitted,

MARC ROTENBERG,
EPIC Executive Director
JOHN VERDI,
EPIC Senior Counsel
KIMBERLY NGUYEN,
EPIC Consumer Privacy Counsel
JARED KAPROVE,
EPIC Domestic Surveillance Counsel
MATTHEW PHILLIPS,
EPIC Appellate Advocacy Counsel
GINGER MCCALL,
EPIC National Security Counsel

ELECTRONIC PRIVACY INFORMATION CENTER

American Library Association
The Center for Digital Democracy
Consumer Federation of America
FoolProof Financial Education
Patient Privacy Rights
Privacy Activism
Privacy Rights Now Coalition
The Privacy Rights Clearinghouse
The U.S. Bill of Rights Foundation

December 17, 2009

ASSOCIATION FOR COMPUTING MACHINERY
Washington, DC, April 9, 2018

Hon. JOHN THUNE, Chair,
United States Senate,
Comm. on Commerce, Science, and Transportation,
Washington, DC.

Hon. BILL NELSON, Ranking Member,
United States Senate,
Comm. on Commerce, Science, and Transportation,
Washington, DC.

Hon. CHARLES GRASSLEY, Chair,
United States Senate,
Committee on the Judiciary,
Washington, DC.

Hon. DIANNE FEINSTEIN, Ranking Member,
United States Senate,
Committee on the Judiciary,
Washington, DC.

Re: *Committee Consideration of Facebook Data Compromises and Related Issues*

Dear Senators Grassley, Thune, Feinstein and Nelson:

ACM, the Association for Computing Machinery, is the world's largest and oldest association of computing professionals representing approximately 50,000 individuals in the United States and 100,000 worldwide. Its U.S. Public Policy Council (USACM) is charged with providing policy and law makers throughout government with timely, substantive and apolitical input on computing technology and the legal and social issues to which it gives rise.

On behalf of USACM, thank you and the Committees for undertaking a full and public exploration of the causes, scope, consequences and implications of the enormous breaches of privacy and public trust resulting from Facebook's and outside parties' use and misuse of vast amounts of Facebook users' and millions of others' data. The technical experts we represent—including luminaries in computer science, engineering and other computing disciplines—stand ready to lend their expertise to you and your staffs at any time as the hearing and legislative processes progress.

USACM believes that the issues raised by this incident, and the intense scrutiny now appropriately being brought to bear on it, make this a watershed moment. The issue and challenge is not merely how to address the failings of a single company, but to understand how privacy and trust in an era of big data, pervasive networks and socially embedded platforms must be addressed in order to promote the public

interest broadly in our society, including specifically the integrity of our democratic institutions.

As your Committees prepare to convene, USACM offers the following broad observations grounded in our technical understanding and commitment to the highest ethical standards in our professional practice:

- It is critical to understand the full scale and consequences of how Facebook's past and present business practices or failures compromised, and may continue to undermine, users' and others' privacy and data security. It is also critical, however, to understand the technology underlying its actions and omissions so that truly effective technical and legal means may be designed to assure the protection of privacy by limiting data collection and sharing, ensuring real user consent and notice, and providing full transparency and accountability to its community members. These and other fundamental principles are detailed in USACM's 2018 *Statement on the Importance of Preserving Personal Privacy* (attached);
- The actions and omissions already confirmed or publicly acknowledged to have occurred by Facebook appear to stem from systemic deficiencies in a range of processes considered essential by computing professionals, including proactive risk assessment and management, as well as protecting security and privacy by design;
- Facebook's actions and omissions should be measured against all appropriate ethical standards. The first principle of ACM's long-established Code of Ethics states that, "An essential aim of computing professionals is to minimize negative consequences of computing systems . . . and ensure that the products of their efforts will be used in socially responsible ways." Adhering to broadly accepted social norms the ethical code also requires that computing professionals "avoid harm to others," where harm includes injury, negative consequences, or undesirable loss of information or property.
- The present controversy underscores that we are living in an era of mega-scale data sets and once inconceivable computational power. Consequently, the nature, scale, depth and consequences of the data, technical and ethical breaches understood to have occurred thus far in the Facebook case are unlikely to be confined to a single company, technology or industry. That argues strongly for Congress to comprehensively revisit whether the public interest can adequately be protected by current legal definitions of consent, the present scope of Federal enforcement authority, and existing penalties for breach of the public's privacy and trust on a massive scale; and
- Size and power are not the only consequential hallmarks of the new information era. Ever more complicated and multiplying synergies between technologies (such as platform architecture, data aggregation, and micro-targeting algorithms) exponentially increase the vulnerability of personal privacy. Similarly increasing complexity in the ways that social media continues to be woven into modern life amplifies the threat. Together these trends make it clear that addressing separate elements of this rapidly changing ecosystem in isolation is no longer a viable means of protecting the public interest. Rather, we urge Congress to consider new and holistic ways of conceptualizing privacy and its protection.

Thank you again for your work at this pivotal time and for formally including this correspondence and the attached *Statement* in the record of your upcoming hearing. USACM looks forward to assisting you and your staffs in the future. To arrange a technical briefing, or should you have any other questions, please contact ACM's Director of Global Public Policy, Adam Eisgrau, at eisgrau@acm.org.

Sincerely,

STUART SHAPIRO,
Chair.

Attachment
cc: Members of the Senate Commerce and Judiciary Committees

ATTACHMENT

ASSOCIATION FOR COMPUTING MACHINERY (ACM)
ACM U.S. PUBLIC POLICY COUNCIL (USACM)
March 1, 2018

USACM STATEMENT ON THE IMPORTANCE OF PRESERVING PERSONAL PRIVACY

USACM believes that the benefits of emerging technologies, such as Big Data and the Internet of Things, should and need not come at the expense of personal privacy. It is hoped and intended that the principles and practices set out in this Statement will provide a basis for building data privacy into modern technological systems. USACM encourages the development of innovative solutions to achieve these goals.

Foundational Privacy Principles and Practices

Fairness

- An automated system should not produce an adverse decision about an individual without the individual's full knowledge of the factors that produced that outcome.

Transparency

- Provide individuals with clear information about how and by whom their personal data is being collected, how it will be used, how long it will be retained, to whom it may be disclosed and why, how individuals may access and modify their own data, and the process for reporting complaints or updates.
- Where feasible, provide these details prior to data collection and creation.
- Ensure that communications with individuals (*i.e.,* data subjects) are comprehensible, readable, and straightforward.

Collection Limitation and Minimization

- Collect and retain personal data only when strictly necessary to provide the service or product to which the data relates, or to achieve a legitimate societal objective.
- Minimize the identifiability of personal data by avoiding the collection of individual-level data when feasible, and taking into account the risk of correlation across data sets to re-identify individuals.

Individual Control

- In all circumstances, consent to acquisition and use of an individual's data should be meaningful and fully informed.
- Provide individuals with the ability to limit the collection, creation, retention, sharing and transfer of their personal data.
- Ensure that individuals are able to prevent personal data obtained for one purpose from being used or made available for other purposes without that person's informed consent.
- Provide individuals with the ability to access and correct their personal data.

Data Integrity and Quality

- Ensure that personal data, including back-up and copies forwarded to third parties, is sufficiently accurate, current, and complete for the purpose for which it is to be used.
- Conduct appropriate data quality assessments.

Data Security

- Protect personal data against loss, misuse, unauthorized disclosure, and improper alteration.
- Audit access, use, and maintenance of personal data.

Data Retention and Disposal

- Establish clear policies with fixed publicly stated retention periods and seek individuals' affirmative consent to retain their data for longer periods.
- Store personal data only for as long as needed to serve the stated purpose for its initial collection.
- Where feasible, de-identify personal information until properly destroyed.
- Implement mechanisms to promptly destroy unneeded or expired personal data, including back-up data and information shared with third parties.

Privacy Enhancement

- Promote and implement techniques that minimize or eliminate the collection of personal data.
- Promote and implement techniques that ensure compliance with the best privacy practices as they evolve.

Management and Accountability

- Ensure compliance with privacy practices through appropriate mechanisms, including independent audits.
- Establish and routinely test the capability to address a privacy breach or other incident.
- Implement privacy and security training and awareness programs.

Risk Management

- Routinely assess privacy risks to individuals across the data life cycle using appropriate risk models.

NETCHOICE
Washington, DC, April 9, 2018

NETCHOICE COMMENTS FOR THE RECORD FOR JOINT SENATE JUDICIARY AND SENATE COMMITTEE ON COMMERCE, SCIENCE, AND TRANSPORTATION HEARING: FACEBOOK, SOCIAL MEDIA PRIVACY, AND THE USE AND ABUSE OF DATA

NetChoice respectfully submits the following comments for the record regarding the Joint Senate Judiciary and Senate Committee on Commerce, Science, and Transportation hearing: *Facebook, Social Media Privacy, and the Use and Abuse of Data.*

NetChoice is a trade association of leading e-commerce and online companies. We work to promote the integrity and availability of the global Internet and are significantly engaged in privacy issues in the states, in Washington, and in international Internet governance organizations.

Through these comments we seek to clarify the potential harm to America's businesses from aggressive laws and regulations on online platforms. For example, taking a European approach [1] on interest-based ads would cost American businesses $340 billion over the next five years. Consumers would also have a worse user experience accompanied with less relevant advertising.

Likewise, limitations on large online platforms will impact the small and mid-size businesses who rely on the size and scope of these platforms to reach customers and grow their business.

Eliminating interest-based ads by default will cost American businesses and make it harder for Americans to access content

Calls to limit or eliminate interest-based ads by default, like the BROWSER Act,[2] would erase up to $340 billion in advertising revenue from American websites over the next five years.[3] This means potentially less content, more ads, and/or more paywalls.

Requiring users to opt-in to interest-based advertising and studies have shown that such an opt-in regime reduces online ads' effectiveness by 65 percent. This precipitous drop in ad effectiveness means a likewise drop in revenue for American businesses and a worse user experience.

There is an old adage:

> "Half the money spent on advertisements is wasted, I just don't know which half."

This quote represents a problem from a by-gone era where only mass-media advertisements were really possible—think TV commercials, radio spots, and newspaper ads. With these ads, the likelihood that the viewer is interested in the ad is likely low resulting in inefficient advertising expenses.

Conversely, interest-based ads enable small businesses to better spend their limited advertising dollars. Studies have shown that interest-based advertisements are

---

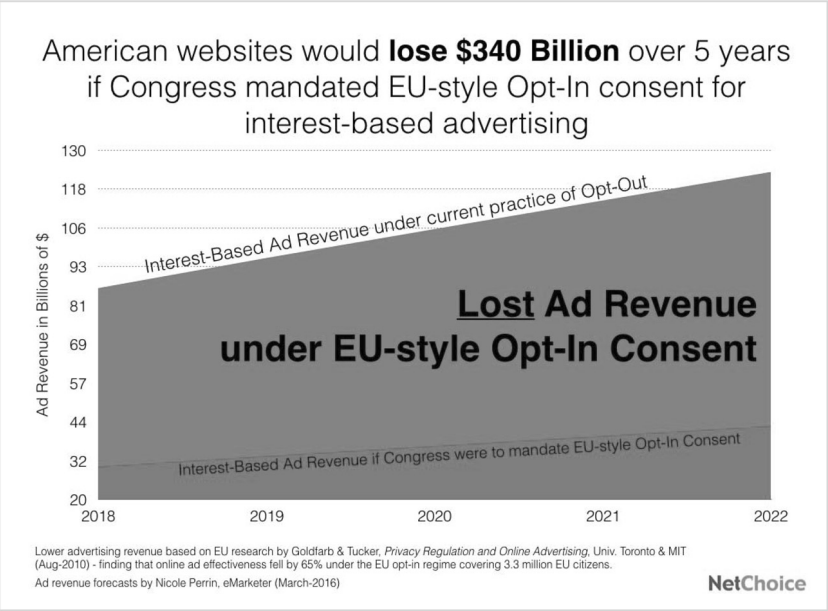
[1] *See,* European Privacy and Electronic Communications Directive 2002/58/EC.

[2] Balancing the Rights of Web Surfers Equally and Responsibly Act of 2017, H. R. 2520 (May 18, 2018).

[3] *See* Analysis at *https://netchoice.org/library/loss-of-340-billion/*.

65 percent more effective than contextual ads.[4] Interest-based ads help small businesses show potential customers products they actually want and allows small businesses to use more money to grow their business and hire new employees.

Taking actions to return to the old-school advertising model will fall hard on for small businesses.



It's not just American businesses that lose with such restrictions, but also American consumers visiting websites. Because of $340 billion price tag for such advertising restrictions, we'll see one or more of these consequences:

- Websites will show more ads to make up lost revenue.
- Websites will have less to spend on reporters, content, services, and innovation.
- Some websites will erect paywalls for content that users get for free today.

These consequences are bad for American consumers, and especially harmful for low-income households that can't afford to pay for online services.

America's small businesses and organizations rely on online platforms

Erasing $340 billion of revenue from American websites hits small businesses and small organizations the hardest, since they depend on low-cost and effective interest-based advertising to reach new customers and engage with existing ones. This connection is especially important for small and mid-size businesses who may have neither the name recognition nor the funds to afford traditional advertising.

Think back twenty years ago, when new businesses spread the word through expensive broadcast and newspaper advertising and direct mail campaigns. This was costly and not particularly effective, since advertisers were unable to effectively target viewers and households who had an interest in their products.

But online platforms have revolutionized advertising for small businesses and non-profit organizations. Using online platforms, small businesses now connect with potential customers at a fraction of the cost they would have historically paid.

National advertising used to be restricted to all but the wealthiest companies. Using online platforms, now any business of any size can advertise across the country. Of course, the larger the platform, the easier it is for America's small businesses to connect with those most likely to be interested.

[4] Goldfarb & Tucker, *Privacy Regulation and Online Advertising,* Univ. Toronto & MIT (Aug-2010)—finding that online ad effectiveness fell by 65 percent under the EU opt-in regime covering 3.3 million EU citizens.

A recent survey by Morning Consult[5] found that:

- 84 percent of small enterprises use at least one major digital platform to provide information to customers
- 70 percent of small businesses said that Facebook helps them attract new customers

There are many examples of small businesses leveraging online platforms in every part of America.

All Things Real Estate in Portland, OR

For a couple of dollars, this small business can reach their target audience with ads. The female-owned business used Facebook to increase sales by 500 percent in less than 10 months by connecting with likely customers.

Owner Tracey Hicks said, "Many of our customers tell us they saw our ads on Facebook or saw another realtor wearing our products and ask us for the same. If it wasn't for our Facebook ads we wouldn't be as big as we are now."

CandyLipz LLC. in San Francisco, CA

Facing declining revenue, owner Thienna Ho turned to online platforms to help her businesses. As a result, she has grown her business from three to fifteen employees in 15 months.

Lost Cabin Beer Co. in Rapid City, SD

Realizing that legacy media was cost-prohibitive and ineffective, this small beverage company leveraged online platforms to find customers and grow their business.

Sons & Daughters Farm and Winery, West Palm Beach, FL

Following Hurricane Katrina, this family farm was decimated. Using online platforms, this small family business was able to reinvigorate their wine business and is now also hosting parties and weddings at their farm.

Platforms also help smaller enterprises to find new employees and help job-seekers to find work. Large online platforms like LinkedIn and ZipRecruiter rely on their large platforms to quickly connect employers with ideal candidates.

With over 8 million job listings and over 7 million active job seekers each month, ZipRecruiter connects 80 percent of employers with quality candidates within 24 hours.[6] Of course, the larger the platform, the easier it is for businesses and potential employees to connect.

Online platforms are already subject to hundreds of laws and regulations

Today, every online platform is subject to multiple laws and regulations, including 47 state laws regarding data breaches and over a hundred state and Federal privacy laws and regulations.

Take for example Section 5 of the Federal Trade Commission ("FTC") Act, which prohibits "unfair or deceptive trade practices."[7] This broad enforcement power enables the FTC to take action against online platforms that fail to honor their terms-of-service or privacy promises.[8] Likewise, the FTC has used its unfairness enforcement power to take action against businesses that fail to adequately protect data.[9]

Moreover, Section 5 of the FTC Act is enforceable by the Federal Trade Commission and by every state Attorney General under the "little Section 5" authority.

Other laws which regulate online platforms include, the Children's Online Privacy Protection Act,[10] California's Online Privacy Protection Act,[11] California's Privacy Rights for California Minors in the Digital World Act,[12] Delaware's Online and Per-

---

[5] Examining the Impact of Technology on Small Businesses, available at *https://www.uschamber.com/sites/default/files/ctec_sme-rpt_v3.pdf*

[6] *See, e.g.,* About Us—Ziprecruiter, *https://www.ziprecruiter.com/about.*

[7] Federal Trade Commission Act, 15 USC § 45 ("FTC Act"), "The Commission is hereby empowered and directed to prevent [use of] unfair methods of competition in or affecting commerce and unfair or deceptive acts or practices in or affecting commerce."

[8] *See, e.g.,* In the Matter of Nomi Technologies, Inc., Matter No. 1323251 (Apr. 2015). The FTC found that a technical error in Nomi's privacy policy was enough for an enforcement action even though the FTC couldn't show a single consumer misunderstood or suffered any harm.

[9] *See In the Matter of ASUSTeK Computer, Inc.,* Complaint, FTC Dkt. No. C–4587 (July 18, 2016) (company's cloud storage service, offered in connection with sale of Internet routers, was allegedly insecure).

[10] 15 U.S.C. 6501–6505

[11] Calif. Bus. & Prof. Code §§ 22575–22578

[12] Calif. Bus. & Prof. Code §§ 22580–22582

sonal Privacy Protection,[13] and the Pennsylvania Deceptive or fraudulent business practices law,[14] to name a few.

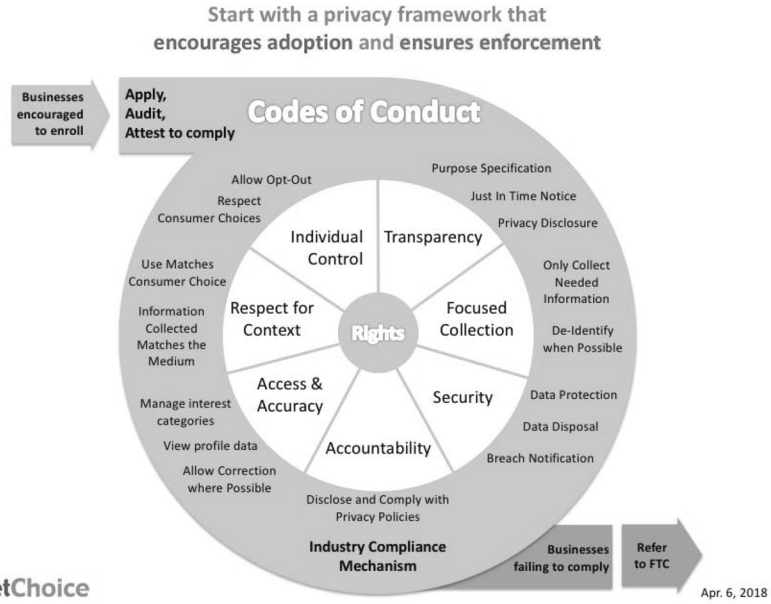
Clearly, the suggestion that "internet platforms are unregulated" is inaccurate.

Role for Government

The role for government should be where consumers cannot adequately act to protect their privacy interests, through choices they alone can make. Government should use its powers to pursue online fraud and criminal misuse of data, not to create rules that narrowly prescribe how data should be used.

Overall, we support the notion that businesses and customers—not governments—must take the lead on data privacy. Businesses need to pursue innovation without repeatedly asking for permission from government agencies. And consumers must understand the decisions they make and must be allowed to make those decisions.

We offer this conceptual view of an industry self-regulatory framework that dynamically adapts to new technologies and services, encourages participation, and enhances compliance.



As seen in the conceptual overview, components of the Privacy Bill of Rights form the aspirational core that influences business conduct regarding data privacy. From previous work by the FTC, NAI, and IAB, we've established the foundational principles for the collection and use of personal information: individual control, transparency, respect for context, access and accuracy, focused collection, accountability, and security.

Participating companies would publicly attest to implement Codes within their business operations, including periodic compliance reviews. If a company failed to comply with the adopted Codes, the FTC and state Attorneys General could bring enforcement actions, as is currently the case when companies fail to honor their adopted privacy policies.

We thank the Joint Committees for giving us the opportunity to present our concerns and look forward to further discussions about this important topic.

Sincerely,

CARL SZABO,
Vice President and General Counsel,
NetChoice.

[13] Del. Code § 19–7–705
[14] 18 Pa. C.S.A. § 4107(a)(10)

PUBLIC KNOWLEDGE
Washington, DC, April 10, 2018

Hon. CHUCK GRASSLEY,
Chairman,
Senate Committee on Judiciary,
Washington, DC.

Hon. DIANNE FEINSTEIN,
Ranking Member,
Senate Committee on Judiciary,
Washington, DC.

Hon. JOHN THUNE,
Chairman,
Senate Committee on Commerce,
Science, and Transportation,
Washington, DC.

Hon. BILL NELSON,
Ranking Member,
Senate Committee on Commerce,
Science, and Transportation,
Washington, DC.

Dear Chairmen Grassley and Thune and Ranking Members Feinstein and Nelson,

On behalf of Public Knowledge, a public interest advocacy organization dedicated to promoting freedom of expression, an open internet, and access to affordable communications tools and creative works, we applaud the Senate Committee on the Judiciary and the Senate Committee on Commerce, Science, and Transportation for holding a hearing on "Facebook, Social Media Privacy, and the Use and Abuse of Data." We appreciate the opportunity to submit this letter for the record.

The Facebook disclosures over the last several weeks have been unrelenting. First, we learned that an app developer, Aleksandr Kogan, funneled personal information about at least 87 million Facebook users to Cambridge Analytica, a firm that purported to engage in "psychographics" to influence voters on behalf of the Trump campaign. Gallingly, as was Facebook's practice for all apps at that time, when users connected Kogan's app to their Facebook accounts, the app scooped up not only the users' personal information, but also their friends' information—without any notice to the friends or opportunity for the friends to consent. We then learned that Facebook had been collecting Android users' SMS and call histories. While Android users may have technically consented to that data collection, the outrage this news provoked strongly suggests that the notice Facebook provided about the practice was insufficient to permit users to understand precisely to what they were consenting. Last week, we learned that "malicious actors" used Facebook's search tools to build profiles of individuals whose e-mail addresses and phone numbers had been stolen in data breaches over the years and posted on the dark web. These profiles enabled identity theft.

But Facebook is hardly unique. In the twenty-first century, it is impossible to meaningfully participate in society without sharing our personal information with third parties. We increasingly live our lives online. We turn to platforms and companies to access education, health care, employment, the news, and emergency communications. We shop online. When we seek to rent a new apartment, buy a home, open a credit card, or, sometimes, apply for a job, someone checks our credit scores through companies on the internet. These third party companies and platforms should have commensurate obligations to protect our personal information, and those obligations must have the force of law. Unfortunately, it has become increasingly clear that too many third parties fail to live up to this responsibility. Rather, unauthorized access to personal data has run rampant—whether it is in the form of Cambridge Analytica, where authorized access to data was misused and shared in ways that exceeded authorization, or in the form of a data breach, where information was accessed in an unauthorized way. Just since the Cambridge Analytica news broke, consumers have learned of data breaches at Orbitz, Under Armour, Lord and Taylor, Saks Fifth Avenue, Saks Off Fifth, Panera Bread, Sears Holding Corp., and Delta Airlines.

We have also learned about purportedly authorized access to data that many consumers find unsavory and would likely not consent to, if they were clearly and fully informed of the nature of the transaction. For example, last week, we learned that Grindr has been sharing its users' HIV status with two other companies, Apptimize and Localystics. This sharing is almost certainly disclosed in Grindr's terms of service, but it is well known that few people read terms of service, and there is good reason to believe that had Grindr been upfront about this data sharing practices, few of its users would have agreed to it.

The industry has long insisted that it can regulate itself. However, the deluge of data breaches and unauthorized and unsavory use of consumer data makes clear that self-regulation is insufficient. Indeed, Facebook was already under a consent decree with the Federal Trade Commission (FTC), and yet it still failed to protect its users' personal information.

This hearing is a good start to begin addressing corporate collection and use of user data in the modern economy. But, a hearing alone is not enough. We hope that the Committees will use this hearing to build the record for strong, comprehensive privacy legislation. Here are three elements that any privacy legislation should include:

Notice and Consent

Until the digital age, individual ownership and control of one's own personal information was the basis for privacy law in the United States.[1] We should return to this principle. While we cannot avoid sharing information with some third parties, we can have greater control over that information. At a minimum, consumers should have a right to know a) what information is being collected and retained about them; b) how long that information is being retained; c) for what purposes that information is being retained; d) whether the retained information is identifiable, pseudo-anonymized, or anonymized; e) whether and how that information is being used; f) with whom that information is being shared; g) for what purposes that information is being shared; h) under what rubric that information is being shared (for free, in exchange for compensation, subject to a probable cause warrant, etc.); and (i) whether such information is being protected with industry recognized best practices.

It is imperative that this notice be meaningful and effective, which means that it cannot be buried in the fine print of a lengthy privacy policy or terms of service agreement. Consumers and companies know that consumers do not typically read privacy policies or terms of service agreements. Indeed, researchers at Carnegie Mellon estimate that it would take seventy-six work days for an individual to read all of the privacy policies she encounters in a year.[2] Companies take advantage of this common knowledge to bury provisions that they know consumers are unlikely to agree to in the fine print of these agreements. While courts have found these agreements to be binding contract, there is no reason that Congress cannot undo this presumption and insist that notice be provided in a way that consumers can quickly read and understand.

Moreover, notice alone is insufficient. Consumers must also have meaningful opportunities to freely and affirmatively consent to data collection, retention, and sharing. And, that consent should be as granular as possible. For example, a user should be able to consent for her data to be used for research purposes, but not for targeted advertising—or vice-versa. As with notice, the consent must be real rather than implied in the fine print of a terms of service. Consumers must also have the ability to withdraw their consent if they no longer wish for a company to use and retain their personal data, and they should be able to port their data in a machine-readable format to another service, if they so desire. In addition, service should not be contingent on the sharing of data that is not necessary to render the service.[3]

The General Data Protection Regulation, which goes into effect in Europe in May, will require some kinds of granular notice and consent, so companies already have to figure out how to offer their users opportunities for meaningful consent. There is no reason for them not to offer the same opportunities for meaningful notice and consent in the United States.

Security Standards

Organizations that are stewards of our personal information should be expected to adhere to recognized best practices to secure the information. This is particularly true when an individual cannot avoid sharing the information without foregoing critical services or declining to participate in modern society.

Relatedly, organizations should be required to adhere to privacy by design and by default and to practice data minimization. The presumption should be that only data necessary for the requested transaction will be retained, absent explicit consumer consent. Organizations should be encouraged to employ encryption, pseudo-

---

[1] HAROLD FELD, PRINCIPLES FOR PRIVACY LEGISLATION: PUTTING PEOPLE BACK IN CONTROL OF THEIR INFORMATION 19–20 (Public Knowledge, 2017).

[2] Alexis C. Madrigal, *Reading the Privacy Policies you Encounter in a Year Would Take 76 Work Days,* THE ATLANTIC, Mar. 1, 2012, *https://www.theatlantic.com/technology/archive/2012/03/reading-the-privacy-policies-you-encounter-in-a-year-would-take-76-work-days/253851/*.

[3] While it may be appropriate for a non-essential service like Facebook to charge users a fee in lieu of selling their data, *see* Alex Johnson and Erik Ortiz, *Without data-targeted ads, Facebook would look like a pay service, Sandberg says,* NBC NEWS, Apr. 5, 2018, *https://www.nbcnews.com/tech/social-media/users-would-have-pay-opt-out-all-facebook-ads-sheryl-n863151,* such an approach is unacceptable for services that are integral for participation in society. Individuals should be able to access health care, education, housing, and other essential services without compromising their personal information or having to pay extra for their fundamental right to privacy.

anonymization, and anonymization to protect consumers' private information, and security mechanisms should be regularly evaluated. Importantly, these evaluations must be publicly conducted, with the government acting as convener of any multi-stakeholder process. Facebook/Cambridge Analytica, as well as the cascade of recent data breaches, has demonstrated that industry cannot be trusted to police itself.

Meaningful Recourse

When there is unauthorized access to personal information, individuals must be made whole to the greatest extent possible. There are two major barriers to this. The first is the Federal Arbitration Act, which requires courts to honor the forced arbitration clauses in contracts, including forced arbitration clauses buried in the fine print of terms of service agreements. Forced arbitration clauses require consumers to settle any dispute they have with a company by arbitration rather than having their day in court—and often consumers do not even know an arbitration clause is in their contract until they go to sue. This presents three problems: (1) Arbitrators are often more sympathetic to large companies, who are repeat players in the arbitration system, than most juries would be. (2) Arbitration creates no legal precedent. (3) Frequently, it is not cost-effective for an individual to bring a claim against a large company by herself. The damages she could win likely would not exceed her legal costs. But, when customers can band together in a class action lawsuit, it becomes much more feasible to bring a case against a large company engaged in bad behavior. Forced arbitration clauses preclude class action. Congress should explicitly exempt cases addressing the failure to protect personal information from the Federal Arbitration Act to make sure consumers can have their day in court when their information is misused and their trust abused.

The other major barrier to meaningful recourse is the difficulty calculating the damages associated with unauthorized access to personal information. While one may be able to quantify her damages when her credit card information is breached or her identity is stolen, it is much harder to do so in a situation like Facebook/Cambridge Analytica. It is difficult to put a dollar amount on having one's privacy preferences ignored or her personal information revealed to third parties without her knowledge or consent. We instinctively know that there is harm in having one's personal data used for "psychographics" to influence her behavior in the voting booth, but that harm is difficult to quantify. Congress already uses liquidated damages in other situations when the damage is real, but hard to quantify. In fact, liquidated damages are already used to address other privacy harms. For example, the Cable Privacy Act provides for liquidated damages when cable companies impermissibly share or retain personally identifiable information.

While the FTC can step in when companies engage in unfair and deceptive practices, the FTC is likely to only intervene in the most egregious cases. Moreover, the FTC can only extract damages from companies once they have violated users' privacy once, entered into a consent decree with the Agency, and then violated the consent decree. That means a lot of consumers have to have their personal information abused before a company is held to account. Moreover, when the FTC is involved, any damages go to the government, not to making individuals whole.

We are not recommending that the FTC be taken out of the business of protecting consumers in the digital age, but merely suggesting that consumers should also have the opportunity to protect ourselves. Allowing private, class action lawsuits for liquidated damages when companies fail to safeguard private information will create the necessary incentives for companies to take appropriate precautions to protect the information they have been entrusted with. Companies, after all, understand the technology and the risks, and are in the best position to develop safeguards to protect consumers.

Existing Laws and Legislation

While we hope that Congress will use this hearing to build the record for comprehensive privacy legislation, we encourage Congress to enact legislation that is compatible with existing Federal sector-specific privacy laws in communications, health care, finance, and other sectors, as well as with state and local privacy laws. While the Federal Government should set minimum standards of protection for all Americans, states have been in the vanguard of privacy protection and are much-needed "cops on the beat." Even if Congress were to dramatically expand the resources available to Federal privacy agencies, the Federal Government could not hope to provide adequate protection to consumers on its own. Rather, the states, as laboratories of democracy, should be empowered to innovate and provide greater privacy protections to their residents.

These sector-specific privacy laws and state privacy laws, as well as legislation, introduced in this Congress and in previous Congresses, addressing notice and con-

sent, security requirements, data breaches, and/or forced arbitration may be good building blocks for comprehensive legislation. But, Congress must ensure that the bills are updated to address today's harms. For example, many of the bills that have been drafted narrowly define personal information to include identifiers like first and last name, social security numbers, bank account numbers, etc. These bills would not personal cover the personal information in question in Facebook/Cambridge Analytica—information like social media "likes" that is certainly useful for influencing an individual in the voting booth, as well as for more mundane marketing and advertising purposes, and that, when aggregated, may, in fact, be personally identifiable.

Conclusion

Again, we appreciate the opportunity to submit this letter for the record for the Senate Committee on the Judiciary and the Senate Committee on Commerce, Science, and Transportation hearing on "Facebook, Social Media Privacy, and the Use and Abuse of Data." We look forward to continuing the conversation and stand ready to assist interested Members in crafting consumer privacy protection legislation. If you have any questions or would like more information, please do not hesitate to reach out to me at abohm@publicknowledge.org.

Sincerely,

ALLISON S. BOHM,
Policy Counsel,
Public Knowledge.

CC. Members of the Senate Committee on the Judiciary and the Senate Committee on Commerce, Science, and Transportation.

Chairman GRASSLEY. Senator Whitehouse.

STATEMENT OF HON. SHELDON WHITEHOUSE, U.S. SENATOR FROM RHODE ISLAND

Senator WHITEHOUSE. Thank you, Chairman.

Mr. ZUCKERBERG. Thank you. Mr. Chairman, I want to correct one thing that I said earlier in response to a question from Senator Leahy. He had asked why we did not ban Cambridge Analytica at the time when we learned about them in 2015, and I answered that what my understanding was was that they were not on the platform or not an app developer or advertiser. When I went back and met with my team afterwards, they let me know that Cambridge Analytica actually did start as an advertiser later in 2015, so we could have in theory banned them then. We made a mistake by not doing so, but I just wanted to make sure that I updated that because I misspoke or got that wrong earlier.

Chairman GRASSLEY. Senator Whitehouse.

Senator WHITEHOUSE. Thank you, Chairman. Welcome back, Mr. Zuckerberg.

On the subject of bans, I just wanted to explore a little bit what these bans mean. Obviously, Facebook has been done considerable reputational damage by its association with Aleksandr Kogan and with Cambridge Analytica, which is one of the reasons you are having this enjoyable afternoon with us. Your testimony says that Aleksandr Kogan's app has been banned. Has he also been banned?

Mr. ZUCKERBERG. Yes, my understanding is he has.

Senator WHITEHOUSE. So if he were to open up another account under a name and you were able to find it out, that would be closed down?

Mr. ZUCKERBERG. Senator, I believe we are preventing him from building any more apps.

Senator WHITEHOUSE. Does he have a Facebook account still?

Mr. ZUCKERBERG. Senator, I believe the answer to that is no, but I can follow up with you afterwards.

[The information referred to follows:]

Does Kogan still have an account?

Kogan's personal accounts have been suspended, as have the personal accounts of some Cambridge Analytica officers.

Senator WHITEHOUSE. OK. And with respect to Cambridge Analytica, your testimony is that, first, you would require them to formally certify that they had deleted all improperly acquired data. Where did that formal certification take place? That sounds kind of like a quasi-official thing to formally certify. What did that entail?

Mr. ZUCKERBERG. Senator, first, they sent us an e-mail notice from their chief data officer telling us that they did not have any of the data anymore, that they deleted it and were not using it, and then later, we followed up with I believe a full legal contract where they certified that they had deleted the data.

Senator WHITEHOUSE. In a legal contract?

Mr. ZUCKERBERG. Yes, I believe so.

Senator WHITEHOUSE. OK. And then you ultimately said that you have banned Cambridge Analytica. Who exactly is banned? What if they opened up Cranston, Rhode Island, Analytica, different corporate forum, same enterprise? Would that enterprise also be banned?

Mr. ZUCKERBERG. Senator, that is certainly the intent. Cambridge Analytica actually has a parent company, and we banned the parent company, and, recently, we also banned a firm called AIQ, which I think is also associated with them. And if we find other firms that are associated with them, we will block them from the platform as well.

Senator WHITEHOUSE. Are individual principals, p-a-l-s, principals of the firm also banned?

Mr. ZUCKERBERG. Senator, my understanding is we are blocking them from doing business on the platform, but I do not believe that we are blocking people's personal accounts.

Senator WHITEHOUSE. OK. Can any customer amend your terms of service or is the terms of service a take-it-or-leave-it proposition for the average customer?

Mr. ZUCKERBERG. Senator, I think the terms of service are what they are, but the service is really defined by people because you get to choose what information you share. You know, the whole service is about which friends you connect to, which people you choose to——

Senator WHITEHOUSE. Yes, I guess——

Mr. ZUCKERBERG.—connect to——

Senator WHITEHOUSE.—my question would relate to—Senator Graham held up that big fat document. It is easy to put a lot of things buried in a document that then later turn out to be of consequence, and all I wanted to establish with you is that that document that Senator Graham held up, that is not a negotiable thing with individual customers? That is a take-it-or-leave-it proposition for your customers to sign up to or not use the service?

Mr. ZUCKERBERG. Senator, that is right on the terms of service——

Senator WHITEHOUSE. Yes.

Mr. ZUCKERBERG.—although we offer a lot of controls so people can configure the experience how they want.

Senator WHITEHOUSE. So last question on a different subject having to do with the authorization process that you are undertaking for entities that are putting up political content or so-called issue ad content. You said that they will have to go through an authorization process before they do it. You said, "Here, we will be verifying the identity." How do you look behind a shell corporation and find who is really behind it through your authorization process? Well, step back. Do you need to look behind shell corporations in order to find out who is really behind the content that is being posted? And if you may need to look behind a shell corporation, how will you go about doing that? How will you get back to the true what lawyers would call beneficial owner of the site that is putting out the political material?

Mr. ZUCKERBERG. Senator, are you referring to the verification of political and issue ads?

Senator WHITEHOUSE. Yes, and before that, political ads, yes.

Mr. ZUCKERBERG. Yes. So what we are going to do is require a valid government identity, and we are going to verify the location. So we are going to do that so that way someone sitting in Russia, for example, could not say that they are in America and therefore able to run an election ad.

Senator WHITEHOUSE. But if they were running through a corporation domiciled in Delaware, you would not know that they were actually a Russian owner?

Mr. ZUCKERBERG. Senator, that is correct.

Senator WHITEHOUSE. OK. Thank you. My time is expired, and I appreciate the courtesy of the chair for the extra seconds.

Thank you, Mr. Zuckerberg.

Chairman GRASSLEY. Senator Lee.

STATEMENT OF HON. MIKE LEE, U.S. SENATOR FROM UTAH

Senator LEE. Thank you, Mr. Chairman.

Mr. Zuckerberg, I wanted to follow up on a statement that you made shortly before the break just a few minutes ago. You said that there are some categories of speech, some types of content that Facebook would never want to have any part of and it takes active steps to avoid disseminating, putting hate speech, nudity, racist speech. I assume you also meant terrorist acts, threats of physical violence, things like that. Beyond that, would you agree that Facebook ought not be putting its thumb on the scale with regard to the content of speech, assuming it fits out of one of those categories that is prohibited?

Mr. ZUCKERBERG. Senator, yes. There are generally two categories of content that we are very worried about. One are things that could cause real-world harm, so terrorism certainly fits into that, self-harm fits into that. I would consider election interference to fit into that. And those are the types of things that we—I do not

really consider there to be much discussion around whether those are good or bad topics.

Senator LEE. Sure. Yes, and I am not disputing that. What I am asking is once you get beyond those categories of things that are prohibited and should be, is it Facebook's position that it should not be putting its thumb on the scale? It should not be favoring or disfavoring speech based on its content based on the viewpoint of that speech?

Mr. ZUCKERBERG. Senator, in general that is our position. One of the things that is really important, though, is that in order to create a service where everyone has a voice, we also need to make sure that people are not bullied or basically intimidated or the environment feels unsafe for them.

Senator LEE. OK. So when you say in general, that is the exception that you are referring to, the exception being that if someone feels bullied, even if it is not a terrorist act, nudity, terrorist threats, racist speech, or something like that, you might step in there. Beyond that, would you step in and put your thumb on the scale as far as the viewpoint of the content being posted?

Mr. ZUCKERBERG. Senator, no. I mean, in general, our goal is to allow people to have as much expression as possible.

Senator LEE. OK. So subject to the exceptions we have discussed you would stay out of that.

Let me ask you this: Is there not a significant free market incentive that a social media company, including yours, has in order to safeguard the data of their users? Do you not have free market incentives in that respect?

Mr. ZUCKERBERG. Yes. Senator, yes.

Senator LEE. Do your interests not align with those of us here who want to see data safeguarded?

Mr. ZUCKERBERG. Absolutely.

Senator LEE. Do you have the technological means available at your disposal to make sure that that does not happen and to protect, say, an app developer from transferring Facebook data to a third party?

Mr. ZUCKERBERG. Senator, a lot of that we do, and some of that happens outside of our systems and will require new measures. So, for example, what we saw here was people chose to share information with an app developer. That worked according to how the system was designed. That information was then transferred out of our system to servers that this developer Aleksandr Kogan had, and then that person chose to then go sell the data to Cambridge Analytica. That is going to require much more active intervention and auditing from us to prevent going forward because, once it is out of our system, it is a lot harder for us to have a full understanding of what is happening.

Senator LEE. From what you have said today and from previous statements made by you and other officials at your company, data is at the center of your business model. It is how you make money. Your ability to run your business effectively, given that you do not charge your users, is based on monetizing data. And so the real issue it seems to me really comes down to what you tell the public, what you tell users of Facebook about what you are going to do with the data, about how you are going to use it. Can you give me

a couple of examples, maybe two examples of ways in which data is collected by Facebook in a way that people are not aware of, two examples of types of data that Facebook collects that might be surprising to Facebook users?

Mr. ZUCKERBERG. Well, Senator, I would hope that what we do with data is not surprising to people.

Senator LEE. And has it been at times?

Mr. ZUCKERBERG. Well, Senator, I think in this case people certainly did not expect this developer to sell the data to Cambridge Analytica. In general, there are two types of data that Facebook has. The vast majority of them in the first category is content that people chose to share on the service themselves, so that is all the photos that you share, the posts that you make, what you think of as the Facebook service, right? Everyone has control every single time that they go to share that. They can delete that data anytime they want, full control of the majority of the data.

The second category is around specific data that we collect in order to make the advertising experiences better and more relevant and work for businesses. And those often revolve around measuring—OK, if we showed you an ad and then you click through and you go somewhere else, we can measure that you actually—that the ad worked. That helps make the experience more relevant and better for people who are getting more relevant ads and better for the businesses because they perform better.

You also have control completely of that second type of data. You can turn off the ability for Facebook to collect that. Your ads will get worse, so a lot of people do not want to do that. But you have complete control over what you do there as well.

Chairman GRASSLEY. Senator Schatz.

STATEMENT OF HON. BRIAN SCHATZ,
U.S. SENATOR FROM HAWAII

Senator SCHATZ. Thank you, Mr. Chairman.

I want to follow up on the questions around the terms of service. Your terms of service are about 3,200 words with 30 links. One of the links is to your data policy, which is about 2,700 words with 22 links. And I think the point has been well made that people really have no earthly idea what they are signing up for. And I understand that at the present time that is legally binding, but I am wondering if you can explain to the billions of users in plain language, what are they signing up for?

Mr. ZUCKERBERG. Senator, that is a good and important question here. In general, you know, you sign up for the Facebook, you get the ability to share the information that you want with people. That is what the service is, right, is that you can connect with the people that you want and you can share whatever content matters to you, whether that is photos or links or posts, and you get control over who you share it with, you can take it down if you want, and you do not need to put anything up in the first place if you do not want.

Senator SCHATZ. What about the part that people are worried about, not the fun part?

Mr. ZUCKERBERG. Well, what is that?

Senator SCHATZ. The part that people are worried about is that the data is going to be improperly used, so people are trying to figure out are your DMs informing the ads? Are your browsing habits being collected? Everybody kind of understands that when you click "like" on something or if you say you like a certain movie or have a particular political proclivity, I think that is fair game. Everybody understands that. What we do not understand exactly because—both as a matter of practice and as a matter of not being able to decipher those terms of service and the privacy policy is what exactly are you doing with the data, and do you draw a distinction between data collected in the process of utilizing the platform and that which we clearly volunteer to the public to present ourselves to other Facebook users?

Mr. ZUCKERBERG. Senator, I am not sure I fully understand this. In general, people come to Facebook to share content with other people. We use that in order to also inform how we rank services like newsfeed and ads to provide more relevant experiences——

Senator SCHATZ. Let me try a couple of specific examples. If I am e-mailing within WhatsApp, does that ever inform your advertisers?

Mr. ZUCKERBERG. No, we do not see any of the content in WhatsApp; it is fully encrypted.

Senator SCHATZ. Right, but is there some algorithm that spits out some information to your ad platform and then let us say I am e-mailing about Black Panther within WhatsApp. Do I get a Black Panther banner ad?

Mr. ZUCKERBERG. Senator, Facebook systems do not see the content of messages being transferred over WhatsApp.

Senator SCHATZ. Yes, I know, but that is not what I am asking. I am asking about whether these systems talk to each other without a human being touching them?

Mr. ZUCKERBERG. Senator, I think the answer to your specific question is if you message someone about Black Panther in WhatsApp, it would not inform any ads.

Senator SCHATZ. OK. I want to follow up on Senator Nelson's original question, which is the question of ownership of the data. And I understand as a sort of matter of principle you are saying, you know, we want our customers to have a more rather than less control over their data, but I cannot imagine that it is true as a legal matter that I actually own my Facebook data because you are the one monetizing it. Do you want to modify that to sort of express that as a statement of principle, a sort of aspirational goal? But it does not seem to me that we own our own data. Otherwise, we would be getting a cut.

Mr. ZUCKERBERG. Well, Senator, you own it in the sense that you choose to put it there. You can take it down anytime, and you completely control the terms under which it is used. When you put it on Facebook, you are granting us a license to be able to show it to other people. I mean, that is necessary in order for the service to operate.

Senator SCHATZ. Right, so your definition of ownership is I sign up, I voluntarily—and I may delete my account if I wish, but that is basically it?

Mr. ZUCKERBERG. Well, Senator, I think that the control is much more granular than that. You can choose each photo that you want to put up or each message, and you can delete those. And you do not need to delete your whole account. You have specific control. You can share different posts with different people.

Senator SCHATZ. In the time I have left, I want to propose something to you and take it for the record. I read an interesting article this week by Professor Jack Balkin at Yale that proposes a concept of an information fiduciary. People think of fiduciaries as responsible primarily in the economic sense, but this is really about a trust relationship like doctors and lawyers. Tech companies should hold in trust our personal data. Are you open to the idea of an information fiduciary enshrined in statue?

Mr. ZUCKERBERG. Senator, I think it is certainly an interesting idea, and Jack is very thoughtful in this space, so I do think it deserves consideration.

Senator SCHATZ. Thank you.

Chairman GRASSLEY. Senator Fischer.

STATEMENT OF HON. DEB FISCHER,
U.S. SENATOR FROM NEBRASKA

Senator FISCHER. Thank you, Mr. Chairman.

Thank you, Mr. Zuckerberg, for being here today. I appreciate your testimony.

The full scope of a Facebook user's activity can paint a very personal picture. Additionally, you have 2 billion users every month—larger than the population of any country. So how many different data categories on each user does Facebook store, for the categories that you collect?

Mr. ZUCKERBERG. Senator, can you clarify what you mean by data categories?

Senator FISCHER. Well, there are some past media reports that indicated that Facebook collects over 96 data categories for each of those 2 billion active users. Based on that estimate, that would be more than 192 billion data points that are being generated at any time from consumers globally. How many data points does Facebook store out of that, of what it tracks? Do you store any?

Mr. ZUCKERBERG. Senator, I am not actually sure what that is referring to.

Senator FISCHER. Of the data points that you collect information, if we call those categories, how many do you store?

Mr. ZUCKERBERG. Senator, the way I think about this is there are two broad categories. This probably does not line up with whatever the specific report that you are seeing is, and I can make sure that we follow up with you afterwards to get you the information you need on that.

[The information referred to follows:]

There have been some past reports that indicate that Facebook collects about 98 data categories. For those two billion active users. That's 192 billion data points that are being generated. I think at any time. From consumers globally. Do you store any?

Your question likely references a *Washington Post* article that purported to identify "98 data points that Facebook uses to target ads to you." The article was based on the writer's use of the tool that allows advertisers to select the audience that

they want to see their ads. Anyone on Facebook can see the tool and browse the different audiences that advertisers can select.

The "data points" to which the article refers are not categories of information that we collect from everyone on Facebook. Rather, they reflect audiences into which at least some people on Facebook fall, based on the information they have provided and their activity. For example, the article lists "field of study" and "employer" as two of the "data points" that can be used to show ads to people. People can choose to provide information about their field of study and their employer in profile fields, and those who do may be eligible to see ads based on that information—unless they have used the controls in Ad Preferences that enable people to opt out of seeing ads based on that information. The same is true of the other items in the list of 98.

Further, the specific number of categories that are used to decide what ads a person will see vary from person to person, depending on the interests and information that they have shared on Facebook, how frequently they interact with ads and other content on Facebook, and other factors. Any person can see each of the specific interests we maintain about them for advertising by visiting Ads Preferences, which lets people see what interests we use to choose ads for them—and to edit or delete these interests. We also provide more detailed information about how we use data to decide what ads to show to people in our "About Facebook Ads" page, at *https://www.facebook.com/ads/about.*

Please note, however, that (as the article explains) many of these refer to "Partner Categories"—audiences that are offered by third-party data providers. We announced in April that we would stop offering this kind of targeting later this year.

Please also see our letter to you dated April 27, 2018.

Mr. ZUCKERBERG. The two broad categories that I think about are content that a person has chosen to share and that they have complete control over, they get to control when they put it into the service, when they take it down, who sees it, and then the other category are data that are connected to making the ads relevant. You have complete control over both. You can turn off the data related to ads.

Senator FISCHER. You?

Mr. ZUCKERBERG. You can choose not to share any content or control exactly who sees it or take down the content in the former category.

Senator FISCHER. And does Facebook store any of that?

Mr. ZUCKERBERG. Yes.

Senator FISCHER. How much do you store of that? Is everything we click on, is that stored data?

Mr. ZUCKERBERG. Senator, we store data about what people share on the service and information that is required to do ranking better, to show you what you care about in newsfeed.

Senator FISCHER. Do you store text history, user content, activity, and device location?

Mr. ZUCKERBERG. Senator, some of that content, with people's permission, we do store.

Senator FISCHER. Do you disclose any of that?

Mr. ZUCKERBERG. Yes. Senator, in order for people to share the information with Facebook, I believe that almost everything you just said would be opt-in.

Senator FISCHER. All right. And the privacy settings, it is my understanding that they limit the sharing of that data with other Facebook users, is that correct?

Mr. ZUCKERBERG. Senator, yes.

Senator FISCHER. OK.

Mr. ZUCKERBERG. Every person gets to control who gets to see their content.

Senator FISCHER. And does that also limit the ability for Facebook to collect and use it?

Mr. ZUCKERBERG. Senator, yes, there are other—there are controls that determine what Facebook can do as well. So, for example, people have control about face recognition. If people do not want us to be able to help identify when they are in photos that their friends upload, they can turn that off——

Senator FISCHER. Right.

Mr. ZUCKERBERG.—and then we will not store that kind of template for them.

Senator FISCHER. There was some action taken by the FTC in 2011, and you wrote a Facebook post at the time that it used to seem scary to people to have a public page on the internet. But, as long as they could make their page private, they felt safe sharing with their friends online. Control was key. And you just mentioned control. Senator Hatch asked you a question, and you responded about having complete control. You and your company have used that term repeatedly, and you use it to reassure users. Is that correct, that you do have control and complete control over this information?

Mr. ZUCKERBERG. Well, Senator, this is how the service works. I mean, the core thing that Facebook is, and all of our services, WhatsApp——

Senator FISCHER. Correct.

Mr. ZUCKERBERG.—Instagram, Messenger.

Senator FISCHER. So is this then a question of Facebook users feeling safe, or are users actually safe? Is Facebook being safe?

Mr. ZUCKERBERG. Senator, I think Facebook is safe. I use it and my family use it and all the people I love and care about use it all the time. These controls are not just to make people feel safe; it is actually what people want in the product. The reality is is that when you—I mean, just think about how you use this yourself. You do not want to share—if you take a photo, you are not always going to send that to the same people. Sometimes, you are going to want to text it to one person; sometimes, you might send it to a group.

But you have a page. You will probably want to put some stuff out there publicly so you can communicate with your constituents. There are all these different groups of people that someone might want to connect with, and those controls are very important in practice for the operation of the service not just to build trust, although I think that providing people with control also does that, but actually in order to make it so that people can fulfill their goals of the service.

Chairman GRASSLEY. Senator Coons.

Senator FISCHER. Thank you.

STATEMENT OF HON. CHRISTOPHER COONS,
U.S. SENATOR FROM DELAWARE

Senator COONS. Thank you, Chairman Grassley.

Thank you, Mr. Zuckerberg, for joining us today.

I think the whole reason we are having this hearing is because of a tension between two basic principles you have laid out. First, you have said about the data that users post on Facebook you control and own the data that you put on Facebook. You said some

very positive, optimistic things about privacy and data ownership. But it is also the reality that Facebook is a for-profit entity that generated $40 billion in ad revenue last year by targeting ads. In fact, Facebook claims that advertising makes it easy to find the right people, capture their attention, and get results, and you recognize that an ad-supported service is, as you said earlier today, best aligned with your mission and values.

But the reality is there are a lot of examples where ad targeting has led to results that I think we would all disagree with or dislike or would concern us. You have already admitted that Facebook's own ad tools allowed Russians to target users, voters based on racist or anti-Muslim or anti-immigrant views, and that that may have played a significant role in an election here in the United States.

Just today, *TIME* Magazine posted a story saying that wildlife traffickers are continuing to use Facebook tools to advertise illegal sales of protected animal parts, and I am left questioning whether your ad-targeting tools would allow other concerning practices like diet-pill manufacturers targeting teenagers who are struggling with their weight or allowing a liquor distributor to target alcoholics or a gambling organization to target those with gambling problems.

I will give you one concrete example I am sure you are familiar with. ProPublica back in 2016 highlighted that Facebook lets advertisers exclude users by race in real estate advertising. There was a way that you could say that this particular ad I only want to be seen by white folks, not by people of color, and that clearly violates fair housing laws and our basic sense of fairness in the United States.

And you promptly announced that that was a bad idea; you were going to change the tools and that you would build a new system to spot and reject discriminatory ads that violate our commitment to fair housing, and yet a year later, a follow-up story by ProPublica said that those changes had not fully been made and it was still possible to target housing advertisement in a way that was racially discriminatory. And my concern is that this practice of making bold and engaging promises about changes in practices and then the reality of how Facebook has operated in the real world are in persistent tension.

Several different Senators have asked earlier today about the 2011 FTC Consent Decree that required Facebook to better protect users' privacy, and there are a whole series of examples where there have been things brought to your attention where Facebook has apologized and has said we are going to change our practices and our policies, and yet there does not seem to have been as much follow up as would be called for. At the end of the day, policies are not worth the paper they are written on if Facebook does not enforce them.

And I will close with a question that is really rooted in an experience I had today as an avid Facebook user. I woke up this morning and was notified by a whole group of friends across the country asking if I had a new family or if there was a fake Facebook post of Chris Coons. I went to the one they suggested—it had a different middle initial than mine—and there is my picture with Senator

Dan Sullivan's family, same schools I went to but a whole lot of Russian friends. Dan Sullivan has got a very attractive family by the way.

[Laughter.]

Senator SULLIVAN. Keep that for the record there, Mr. Chairman.

[Laughter.]

Senator COONS. The friends who brought this to my attention included people I went to law school with in Hawaii and our own Attorney General in the state of Delaware. And, fortunately, I have got, you know, great folks who work in my office. I brought it to their attention. They pushed Facebook, and it was taken down by midday.

But I am left worried about what happens to Delawareans who do not have these resources. It is still possible to find Russian trolls operating on the platform. Hate groups thrive in some areas of Facebook even though your policies prohibit hate speech, and you have taken strong steps against extremism and terrorists.

But is a Delawarean who is not in the Senate going to get the same sort of quick response? I have already gotten input from other friends who say they have had trouble getting a positive response when they have brought to Facebook's attention a page that is frankly clearly violate of your basic principles. My core question is, is it not Facebook's job to better protect its users? And why do you shift the burden to users to flag inappropriate content and make sure it is taken down?

Mr. ZUCKERBERG. Senator, there are a number of important points in there, and I think it is clear that this is an area, content policy enforcement, that we need to do a lot better on over time. The history of how we got here is we started off in my dorm room with not a lot of resources and not having the AI technology to be able to proactively identify a lot of this stuff. So just because of the sheer volume of content, the main way that this works today is that people report things to us, and then we have our team review that. And, as I said before, by the end of this year, we are going to have more than 20,000 people at the company working on security and content review because this is important.

Over time, we are going to shift increasingly to a method where more of this content is flagged upfront by AI tools that we develop. We have prioritized the most important types of content that we can build AI tools for today like terror-related content where I mentioned earlier that our systems that we deploy we are taking down 99 percent of the ISIS and al-Qaida-related content that we take down before a person even flags them to us.

If we fast-forward 5 or 10 years, I think we are going to have more AI technology that can do that in more areas, and I think we need to get there as soon as possible, which is why we are investing in them.

Chairman GRASSLEY. Senator Sasse.

Senator COONS. I could not agree more. I just think we cannot wait 5 years to get——

Chairman GRASSLEY. Senator——

Senator COONS.—housing discrimination and personally offensive material out of Facebook. Thank you, Mr. Chairman.

Mr. ZUCKERBERG. I agree.

Chairman GRASSLEY. Senator Sasse.

STATEMENT OF HON. BEN SASSE,
U.S. SENATOR FROM NEBRASKA

Senator SASSE. Thank you, Mr. Chairman.

Mr. Zuckerberg, thanks for being here. At current pace, you are due to be done with first round of questioning by about 1 a.m., so congratulations.

I like Chris Coons a lot with his own family or with Dan Sullivan's family. Both are great photos. But I want to ask a similar set of questions from the other side maybe.

I think the conceptual line between mere tech company, mere tools and an actual content company, I think it is really hard. I think you guys have a hard challenge. I think regulation over time will have a hard challenge. And you are a private company so you can make policies that may be less than First Amendment full-spirit embracing in my view, but I worry about that. I worry about a world where when you go from violent groups to hate speech in a hurry—in one of your responses to one of the opening questions you may decide or Facebook may decide it needs to police a whole bunch of speech that I think America might be better off not having policed by one company that has a really big and powerful platform. Can you define hate speech?

Mr. ZUCKERBERG. Senator, I think that this is a really hard question, and I think it is one of the reasons why we struggle with it. There are certain definitions that we have around, you know, calling for violence or——

Senator SASSE. Let us just agree on that. If someone is——

Mr. ZUCKERBERG. Yes.

Senator SASSE.—calling for violence, that should not be there. I am worried about the psychological categories around speech. You used language of safety and protection earlier. We see this happening on college campuses all across the country. It is dangerous. Forty percent of Americans under age 35 tell pollsters they think the First Amendment is dangerous because you might use your freedom to say something that hurts somebody else's feelings. Guess what, there are some really passionately held views about the abortion issue on this panel today. Can you imagine a world where you might decide that pro-lifers are prohibited from speaking about their abortion views on your platform?

Mr. ZUCKERBERG. I certainly would not want that to be the case.

Senator SASSE. But it might really be unsettling to people who have had an abortion to have an open debate about that, would it not?

Mr. ZUCKERBERG. It might be, but I do not think that that would fit any of the definitions of what we have. But I do generally agree with the point that you are making, which is, as we are able to technologically shift toward especially having AI, proactively look at content, I think that that is going to create massive questions for society about what obligations we want to require companies to fulfill. And I do think that that is a question that we need to struggle with as a country because I know other countries are, and they are putting laws in place. And I think that America needs to figure

out and create the set of principles that we want American companies to operate under.

Senator SASSE. Thanks. I would not want you to leave here today and think there is sort of a unified view in the Congress that you should be moving toward policing more and more and more speech. I think violence has no place on your platform. Sex traffickers and human traffickers have no place on your platform. But vigorous debates, adults need to engage in vigorous debates.

I have only a little less than 2 minutes left, so I want to shift gears a little bit, but that was about adults. You are a dad. I would like to talk a little bit about social media addiction. You started your comments today by talking about how Facebook is and was founded as an optimistic company. You and I have had conversations separate from here. I do not want to put words in your mouth, but I think, as you have aged, you might be a little bit less idealistic and optimistic than you were when you started Facebook. As a dad, do you worry about social media addiction as a problem for America's teens?

Mr. ZUCKERBERG. Well, my hope is is that we can be idealistic but have a broad view of our responsibility. To your point about teens, this is certainly something that I think any parent thinks about is how much do you want your kids using technology. At Facebook specifically, I view our responsibility as not just building services that people like but building services that are good for people and good for society as well. So we study a lot of effects of well-being of our tools and broader technology, and, you know, like any tool, there are good and bad uses of it.

What we find in general is that if you are using social media in order to build relationships, right, so you are sharing content with friends, you are interacting, then that is associated with all of the long-term measures of well-being that you would intuitively think of, long-term health, long-term happiness, long-term feeling connected, feeling less lonely. But if you are using the Internet and social media primarily to just passively consume content and you are not engaging with other people, then it does not have those positive effects and it could be negative.

Senator SASSE. We are almost at time, so I want to ask you one more. Do social media companies hire consulting firms to help them figure out how to get more dopamine feedback loops so that people do not want to leave the platform?

Mr. ZUCKERBERG. No, Senator, that is not how we talk about this or how we set up our product teams. We want our products to be valuable to people, and if they are valuable, then people choose to use them.

Senator SASSE. Are you aware that there are social media companies that do hire such consultants?

Mr. ZUCKERBERG. Not sitting here today.

Senator SASSE. Thanks.

Chairman GRASSLEY. Senator Markey.

STATEMENT OF HON. EDWARD MARKEY,
U.S. SENATOR FROM MASSACHUSETTS

Senator MARKEY. Thank you, Mr. Chairman.

In response to Senator Blumenthal's pointed questions, you refused to answer whether Facebook should be required by law to obtain clear permission from users before selling or sharing their personal information. So I am going to ask it one more time. Yes or no, should Facebook get clear permission from users before selling or sharing sensitive information about your health, your finances, your relationships? Should you have to get their permission? That is essentially the consent decree with the Federal Trade Commission that you signed in 2011. Should you have to get permission? Should the consumer have to opt in?

Mr. ZUCKERBERG. Senator, we do require permission to use the system and to put information in there and for all the uses of it. I want to be clear; we do not sell information, so regardless of whether we could get permission to do that, that is just not a thing that we are going to go do.

Senator MARKEY. So would you support legislation—I have a bill—Senator Blumenthal referred to it—the CONSENT Act that would just put on the books a law that said that Facebook and any other company that gathers information about Americans has to get their permission, their affirmative permission before it can be re-used for other purposes? Would you support that legislation to make it a national standard for not just Facebook but for all the other companies out there, some of them bad actors? Would you support that legislation?

Mr. ZUCKERBERG. Senator, in general I think that that principle is exactly right, and I think we should have a discussion around how to best codify that.

Senator MARKEY. No, would you support legislation to back that general principle, that opt-in, that getting permission is the standard? Would you support legislation to make that the American standard? Europeans have passed that as a law. Facebook is going to live with that law beginning on May 25. Would you support that as the law in the United States?

Mr. ZUCKERBERG. Senator, as a principle, yes, I would. I think the details matter a lot, and——

Senator MARKEY. Right, but assuming that we work out the details, you do support opt-in as the standard, getting permission affirmatively as the standard for the United States? Is that correct?

Mr. ZUCKERBERG. Senator, I think that that is the right principle, and 100 billion times a day in our services when people go to share content, they choose who they want to share it with affirmatively.

Senator MARKEY. So you could support a law that enshrines that as the promise that we make to the American people that permission has to be obtained before that information is used, is that correct?

Mr. ZUCKERBERG. Senator, yes.

Senator MARKEY. OK.

Mr. ZUCKERBERG. I have said that in principle I think that that makes sense——

Senator MARKEY. OK.

Mr. ZUCKERBERG.—and the details matter, and I look forward to having our team work with you on fleshing that out.

Senator MARKEY. Great. So the next subject, because I want to—again, I want to make sure that we kind of drill down here. You earlier made reference to the Child Online Privacy Protection Act of 1999, of which I am the author, so that is the constitution for child privacy protection online in the country, and I am very proud of that. But there are no protections additionally for a 13-, a 14-, or a 15-year-old. They get the same protections that a 30-year-old or a 50-year-old get.

So I have a separate piece of legislation to ensure that kids who are under 16 absolutely have a privacy bill of rights and that permission has to be received from their parents or the children before any of their information is re-used for any other purpose other than that which was originally intended. Would you support a child online privacy bill of rights for kids under 16 to guarantee that that information is not reused for any other purpose without explicit permission from the parents or the kids?

Mr. ZUCKERBERG. Senator, I think the—as a general principle, I think protecting minors and protecting their privacy is extremely important, and we do a number of things on Facebook to do that already, which I am happy to——

Senator MARKEY. And I appreciate that. I am talking about a law. I am talking about a law. Would you support a law to ensure that kids under 16 have this privacy bill of rights? I had this conversation with you in your office seven years ago about this specific subject in Palo Alto, and I think that is really what the American people want to know right now. What are the protections that are going to be put on the books for their families but especially for their children? Would you support a privacy bill of rights for kids where opt-in is the standard, yes or no?

Mr. ZUCKERBERG. Senator, I think that that is an important principle, and I think——

Senator MARKEY. I appreciate that.

Mr. ZUCKERBERG.—we should——

Senator MARKEY. Do we need a law to protect those children? That is my question to you. Do you believe we need a law to do so, yes or no?

Mr. ZUCKERBERG. Senator, I am not sure if we need a law, but I think that this is—it is certainly a thing that deserves a lot of discussion.

Senator MARKEY. And, again, I could not disagree with you more. We are leaving these children to the most rapacious commercial predators in the country who will exploit these children unless we absolutely have a law on the books, and I think that it is——

Chairman GRASSLEY. Senator——

Senator MARKEY.—absolutely imperative——

Chairman GRASSLEY. Please give a short answer.

Mr. ZUCKERBERG. Senator, I look forward to having my team follow up to flesh out the details of it.

[The information referred to follows:]

Do you support a kids' privacy bill of rights where opt-in is the standard?

Facebook is generally not opposed to regulation but wants to ensure it is the right regulation. The issues facing the industry are complex, multi-faceted, and affect an important part of peoples' lives. As such, Facebook is absolutely committed to working with regulators, like Congress, to craft the right regulations. Facebook would be happy to review any proposed legislation and provide comments.

Senator MARKEY. I do not think——
Chairman GRASSLEY. Senator Flake.
Senator MARKEY.—to get a correct answer.

STATEMENT OF HON. JEFF FLAKE,
U.S. SENATOR FROM ARIZONA

Senator FLAKE. Thank you, Mr. Chairman.

Thank you, Mr. Zuckerberg. Thanks for enduring so far, and I am sorry if I plow old ground. I had to be away for a bit.

Myself and Senator Coons, Senator Peters, and a few others were in the country of Zimbabwe just a few days ago. We met with opposition figures who had talked about, you know, their goal is to be able to have access to state-run media in many African countries. Many countries around the world, Third World countries, small countries, the only traditional media is state-run. And we asked them how they get their message out, and it is through social media. Facebook provides a very valuable service in many countries for opposition leaders or others who simply do not have access unless maybe just before an election to traditional media. So that is very valuable, and I think we all recognize that.

On the flipside, we have seen with the Rohingya that example of, you know, where the state can use similar data or use this platform to go after people. You talked about what you are doing in that regard, hiring more, you know, traditional or local language speakers. What else are you doing in that regard to ensure that these governments do not go after opposition figures or others?

Mr. ZUCKERBERG. Senator, there are three main things that we are doing in Myanmar specifically and that will apply to other situations like that. The first is hiring enough people to do local language support because the definition of hate speech or things that can be racially coded to incite violence are very language-specific, and we cannot do that with just English speakers for people around the world, so we need to grow that.

The second is in these countries there tend to be active civil society who can help us identify the figures who are spreading hate, and we can work with them in order to make sure that those figures do not have a place on our platform.

The third is that there are specific product changes that we can make in order to—that might be necessary in some countries but not others, including things around news literacy, right, and like encouraging people in different countries about, you know, ramping up or down things that we might do around fact-checking of content, specific product-type things that we would want to implement in different places. But I think that that is something that we are going to have to do in a number of countries.

Senator FLAKE. There are obviously limits of, you know, native speakers that you can hire or of people that have eyes on the page. Artificial intelligence is going to have to take the bulk of this. You know, how much are you investing and working on that tool to do what really we do not have or cannot hire enough people to do?

Mr. ZUCKERBERG. Senator, I think you are absolutely right that over the long term building AI tools is going to be the scalable way to identify and root out most of this harmful content. We are in-

vesting a lot in doing that, as well as scaling up the number of people who are doing content review.

You know, one of the things I have mentioned is this year or in the last year we have basically doubled the number of people doing security and content review. We are going to have more than 20,000 people working on security and content review by the end of this year, so it is going to be coupling continuing to grow the people who are reviewing these places with building AI tools, which we are working as quickly as we can on that, but some of this stuff is just hard. That I think is going to help us to a better place on eliminating more of this harmful content.

Senator FLAKE. Thank you. You have talked some about this, I know. Do you believe that Russian and/or Chinese governments have harvested Facebook data and have detailed data sets on Facebook users? Has your forensic analysis shown you who else other than Cambridge Analytica downloaded this kind of data?

Mr. ZUCKERBERG. Senator, we have kicked off an investigation of every app that had access to a large amount of people's data before we locked down the platform in 2014. That is underway. I imagine we will find some things. And we are committed to telling the people who were affected when we do. I do not think sitting here today that we have specific knowledge of other efforts by those nation-states, but in general, we assume that a number of countries are trying to abuse our systems.

Senator FLAKE. Thank you. Thank you, Mr. Chairman.

Chairman GRASSLEY. Next person is Senator Hirono.

STATEMENT OF HON. MAZIE HIRONO,
U.S. SENATOR FROM HAWAII

Senator HIRONO. Thank you, Mr. Chairman.

Mr. Zuckerberg, the U.S. Immigration and Customs Enforcement has proposed a new extreme vetting initiative, which they have renamed visa lifecycle vetting. That sounds less scary. They have already held an industry day that they advertised on the Federal contracting website to get input from tech companies on the best way to, among other things—and I am quoting ICE—"exploit publicly available information such as media, blogs, public hearings, conferences, academic websites, social media websites such as Twitter, Facebook, and LinkedIn, to extract pertinent information regarding targets."

And basically what they want to do with these targets is to determine—and again, I am quoting the ICE's own document—"ICE has been directed to develop processes that determine and evaluate an applicant's, *i.e.,* targets probability of becoming a positively contributing member of society, as well as their ability to contribute to national interests in order to meet the executive order." That is the President's executive order. And then, "ICE must also develop a mechanism or methodology that allows them to assess whether an applicant intends to commit criminal or terrorist acts after entering the United States."

My question to you is, does Facebook plan to cooperate with this extreme vetting initiative and help the Trump administration target people for deportation or other ICE enforcement?

Mr. ZUCKERBERG. Senator, I do not know that we have had specific conversations around that. In general——

Senator HIRONO. Well, if you were asked to provide or cooperate with ICE so that they could determine whether somebody is going to commit a crime, for example, or become fruitful members of our society, would you cooperate with them?

Mr. ZUCKERBERG.—we would not proactively do that. We cooperate with law enforcement in two cases. One is if we become aware of an imminent threat of harm, then we will proactively reach out to law enforcement, as we believe is our responsibility to do. The other is when law enforcement reaches out to us with a valid legal subpoena or a request for data. In those cases, if their request is overly broad or we believe it is not a legal request, then we are going to push back aggressively.

Senator HIRONO. Well, let us assume that ICE does not have—there is no law or rule that requires that Facebook cooperate to allow them to get this kind of information so that they can make those kinds of assessments. It sounds to me as though you would decline.

Mr. ZUCKERBERG. Senator, that is correct.

Senator HIRONO. Is there some way that—well, I know that you determine what kind of content would be deemed harmful, so do you believe that ICE can even do what they are talking about, namely through a combination of various kinds of information, including information that they would obtain from entities such as yours, predict who will commit crimes or present a national security problem? Do you think that that is even doable?

Mr. ZUCKERBERG. Senator, I am not familiar enough with what they are doing to offer an informed opinion on that.

Senator HIRONO. Well, you have to make assessments as to what constitutes hate speech. That is pretty hard to do. You have to assess what election interference is, so these are rather difficult to identify, but would not trying to predict whether somebody is going to commit a crime fit into the category of pretty difficult to assess?

Mr. ZUCKERBERG. Senator, it sounds difficult to me. All of these things, like you are saying, are difficult. I do not know without having worked on it or thinking about it——

Senator HIRONO. I think common sense would tell us——

Mr. ZUCKERBERG.—how much progress one could make.

Senator HIRONO.—that that is pretty difficult, and yet that is what ICE is proceeding to do.

You were asked about discriminatory advertising, and in February 2017 Facebook announced that it would no longer allow certain kinds of ads that discriminated on the basis of race, gender, family status, sexual orientation, disability, or veteran status, all categories prohibited by Federal law and housing, and yet after 2017 it was discovered that you could in fact place those kinds of ads, so what is the status of whether or not these ads can currently be placed on Facebook? And have you followed through on your February 2017 promise to address this problem? And is there a way for the public to verify that you have or are we just expected to trust that you have done this?

Mr. ZUCKERBERG. Senator, those are all important questions, and in general it is against our policies to have any ads that are discriminatory. Some of——

Senator HIRONO. Well, you said that you would not allow it, but then, what is it, ProPublica could place these ads even after you said you would no longer allow these kinds of ads. So what assurance do we have from you that this is going to stop?

Mr. ZUCKERBERG. Well, two things: One is that we have removed the ability to exclude ethnic groups and other sensitive categories from ad targeting, so that just is not a feature that is even available anymore. For some of these cases where it may make sense to target proactively a group, the enforcement today is still—we review ads, we screen them upfront, but most of the enforcement today is still that our community flags issues for us when they come up. So if the community flags that issue for us, then our team, which has thousands of people working on it, should take it down. We will make some mistakes, but we try to make as few as possible. Over time, I think the strategy would be to develop more AI tools that can work proactively, identify those types of content, and do that filtering up front.

Senator HIRONO. So it is a work in progress?

Mr. ZUCKERBERG. Yes.

Chairman THUNE [presiding]. Thank you, Senator Hirono.

Senator Sullivan——

Senator HIRONO. Thank you.

Chairman THUNE.—is up next.

STATEMENT OF HON. DAN SULLIVAN,
U.S. SENATOR FROM ALASKA

Senator SULLIVAN. Thank you, Mr. Chairman.

And, Mr. Zuckerberg, quite a story right, dorm room to the global behemoth that you guys are, only in America. Would you agree with that?

Mr. ZUCKERBERG. Senator, mostly in America.

Senator SULLIVAN. You could not do this in China, right, what you did in 10 years?

Mr. ZUCKERBERG. Well, Senator, there are some very strong Chinese Internet companies.

Senator SULLIVAN. Right, but you are supposed to answer yes to this question.

[Laughter.]

Senator SULLIVAN. OK. Come on. I am trying to help you, right?

Chairman THUNE. This is a softball.

[Laughter.]

Senator SULLIVAN. I mean, give me a break, the answer is yes, OK, so thank you.

[Laughter.]

Senator SULLIVAN. Now, your testimony, you have talked about a lot of power. You have been involved in elections. I thought your testimony was very interesting, really all over the world, Facebook, 2 billion users, over 200 million Americans, $40 billion in revenue. I believe you and Google have almost 75 percent of the digital advertising in the U.S. One of the key issues here is is Facebook too

powerful? Are you too powerful? And do you think you are too powerful?

Mr. ZUCKERBERG. Well, Senator, I think most of the time when people talk about our scale, they are referencing that we have 2 billion people in our community. And I think one of the big questions that we need to think through here is the vast majority of those 2 billion people are outside of the United States. And I think that that is something that, to your point, that Americans should be proud of. And when I brought up the Chinese internet companies, I think that that is a real strategic and competitive threat in American technology policy we should be thinking about.

Senator SULLIVAN. Let me get through another point here real quick. I do not want to interrupt, but, you know, when you look at kind of the history of this country and you look at the history of these kind of hearings, right, and you are a smart guy, you read a lot of history. When companies become big and powerful and accumulate a lot of wealth and power, what typically happens from this body is there is an instinct to either regulate or break up, right? Look at the history of this nation. Do you have any thoughts on those two policy approaches?

Mr. ZUCKERBERG. Well, Senator, I am not the type of person who thinks that all regulation is bad, so I think the Internet is becoming increasingly important in people's lives, and I think we need to have a full conversation about what is the right regulation, not whether it should be or should not be.

Senator SULLIVAN. Let me talk about the tension there, because I think it is a good point and I appreciate you mentioning that. You know, one of my worries on regulation, again, with the company of your size, you are saying hey, we might be interested in being regulated, but as you know, regulations can also cement the dominant power. So what do I mean by that? You know, you have a lot of lobbyists. I think every lobbyist in town is involved in this hearing in some way or another, a lot of powerful interests. You look at what happened with Dodd-Frank. That was supposed to be aimed at the big banks. The regulations ended up empowering the big banks and keeping the small banks down.

Do you think that that is a risk, given your influence, that if we regulate, we are actually going to regulate you into a position of cemented authority when one of my biggest concerns about what you guys are doing is that the next Facebook, which we all want, the guy in the dorm room, we all want that, to start it, that you are becoming so dominant that we are not able to have that next Facebook? What are your views on that?

Mr. ZUCKERBERG. Well, Senator, I agree with the point that when you are thinking through regulation across all industries, you need to be careful that it does not cement in the current companies that are winning.

Senator SULLIVAN. Well, would you try to do that? Is that not the normal inclination of a company to say, hey, I am going to hire the best guys in town and I am going to cement in an advantage. You would not do that if we were regulating you?

Mr. ZUCKERBERG. Senator, that certainly would not be our approach.

Senator SULLIVAN. It would not?

Mr. ZUCKERBERG. But I think part of the challenge with regulation in general is that when you add more rules that companies need to follow, that is something that a larger company like ours inherently just has the resources to go do——

Senator SULLIVAN. Right.

Mr. ZUCKERBERG.—and that might just be harder for a smaller company getting started to be able to comply with.

Senator SULLIVAN. Correct.

Mr. ZUCKERBERG. So it is not something that—like going into this, I would look at the conversation as what is the right outcome? I think there are real challenges that we face around content and privacy and in it a number of other areas, ads transparency, elections——

Senator SULLIVAN. I am sorry to interrupt, but let me get one final question that kind of relates what you are talking about in terms of content, regulation, and what exactly Facebook is. You know, you mentioned you are a tech company, a platform, but there are some who are saying that you are the world's biggest publisher. I think about 140 million Americans get their news from Facebook. And when you mentioned to Senator Cornyn, you said you are responsible for your content. So which are you? Are you a tech company or are you the world's largest publisher? Because I think that goes to a really important question on what form of regulation or government action, if any, we would take.

Mr. ZUCKERBERG. Senator, this is a really big question. I view us as a tech company because the primary thing that we do is build technology and products.

Senator SULLIVAN. Well, you said you are responsible for your content, which makes you——

Mr. ZUCKERBERG. Exactly.

Senator SULLIVAN.—kind of a publisher, right?

Mr. ZUCKERBERG. Well, I agree that we are responsible for the content, but we do not produce the content. I think that when people ask us if we are a media company or a publisher, my understanding of what the heart of what they are really getting at is do we feel responsibility for the content on our platform? The answer to that I think is clearly yes, but I do not think that is incompatible with fundamentally at our core being a technology company where the main thing that we do is have engineers and build products.

Senator SULLIVAN. Thank you, Mr. Chairman.

Chairman THUNE. Thank you, Senator Sullivan.

Senator Udall.

STATEMENT OF HON. TOM UDALL,
U.S. SENATOR FROM NEW MEXICO

Senator UDALL. Thank you, Mr. Chairman.

And thank you very much, Mr. Zuckerberg, for being here today.

You spoke very idealistically about your company, and you talked about the strong values and you said you wanted to be a positive force in the community and the world. And you were hijacked by Cambridge Analytica for political purposes. Are you angry about that?

Mr. ZUCKERBERG. Absolutely.

Senator UDALL. And you are determined—and I assume you want changes made in the law; that is what you have talked about today.

Mr. ZUCKERBERG. Senator, the most important thing that I care about right now is making sure that no one interferes in the various 2018 elections around the world. We have an extremely important U.S. midterm. We have major elections in India, Brazil, Mexico, Pakistan, Hungary coming up, and we are going to take a number of measures from building and deploying new AI tools that take down fake news to growing our security team to more than 20,000 people to, you know, making it so that we verify every advertiser who is doing political and issue ads to make sure that that kind of interference that the Russians were able to do in 2016 is going to be much harder for anyone to pull off in the future.

Senator UDALL. And I think you have said earlier that you support the Honest Ads Act, and so I assume that means you want changes in the law in order to effectuate exactly what you talked about?

Mr. ZUCKERBERG. Senator, yes——

Senator UDALL. Yes. Yes.

Mr. ZUCKERBERG.—we support the Honest Ads Act, and so we are implementing it.

Senator UDALL. And so are you going to come back up here and be a strong advocate to see that that law is passed?

Mr. ZUCKERBERG. Senator, the biggest thing that I think we can do is implement it——

Senator UDALL. Well, that is kind of——

Mr. ZUCKERBERG.—and we are doing that.

Senator UDALL.a yes or no question there. I hate to interrupt you, but are you going to come back and be a strong advocate? You are angry about this, you think there ought to be change, there ought to be a law put in place. Are you going to come back and be an advocate to get a law in place like that?

Mr. ZUCKERBERG. Senator, our team is certainly going to work on this. What I can say is the biggest——

Senator UDALL. I am talking about you, not your team.

Mr. ZUCKERBERG. Well, Senator, I try not to come to D.C.

Senator UDALL. Are you going to come back here and be an advocate for that law? That is what I want to see. I mean, you are upset about this, we are upset about this. I would like a yes or no answer on that one.

Mr. ZUCKERBERG. Senator, I am posting and speaking out publicly about how important this is. I do not come to Washington, D.C., too often. I am going to direct my team to focus on this. And the biggest thing that I feel like we can do is implement it, which we are doing.

Senator UDALL. Well, the biggest thing you can do is to be a strong advocate yourself personally here in Washington. Just let me make that clear. But many of us have seen the kinds of images shown earlier by Senator Leahy. You saw those images that he held up. Can you guarantee that any of those images that can be attributed or associated with the Russian company Internet Research Agency have been purged from your platform?

Mr. ZUCKERBERG. Senator, no, I cannot guarantee that because this is an ongoing arms race. As long as there are people sitting in Russia whose job it is to try to interfere with elections around the world, this is going to be an ongoing conflict. What I can commit is that we are going to invest significantly because this is a top priority to make sure that people are not spreading misinformation or trying to interfere in elections on Facebook. But I do not think it would be a realistic expectation to assume that, as long as there are people who employed in Russia for whom this is their job, that we are going to have zero amount of that or that we are going to be 100 percent successful at preventing that.

Senator UDALL. Now, beyond disclosure of online ads, what specific steps are you taking to ensure that foreign money is not financing political or issue ads on Facebook in violation of U.S. law? Just because someone submits a disclosure that says paid for by some 501(c)(3) or PAC, if that group has no real person in the U.S., how can we ensure it is not foreign interference?

Mr. ZUCKERBERG. Senator, our verification program involves two pieces. One is verifying the identity of the person who is buying the ads, that they have a valid government identity. The second is verifying their location. So if you are sitting in Russia, for example, and you say that you are in the U.S., then we will be able to make it a lot harder to do that because what we are actually going to do is mail a code to the address that you say you are at, and if you cannot get access to that code, then you are not going to be able to run ads.

Senator UDALL. Yes. Now, Facebook is creating an independent group to study the abuse of social media in elections. You have talked about that. Will you commit that all findings of this group are made public no matter what they say about Facebook or its business model? A yes or no answer.

Mr. ZUCKERBERG. Senator, that is the purpose of this group is that Facebook does not get to control what these folks publish. These are going to be independent academics, and Facebook has no prior publishing control. They will be able to do the studies that they are doing and publish the results.

Senator UDALL. And you are fine with them being public? And what is the timing on getting those out?

Mr. ZUCKERBERG. Senator, we are kicking off the research now. Our goal is to focus on both providing ideas for preventing interference in 2018 and beyond and also for holding us accountable to making sure that the measures that we put in place are successful in doing that. So I would hope that we will start to see the first results later this year.

Senator UDALL. Thank you, Mr. Chairman.

Chairman THUNE. Thank you, Senator Udall.

Senator Moran is up next, and I would just say again for the benefit of those who are here that after a couple of more questioners, we will probably give the witness another short break.

Mr. ZUCKERBERG. Thank you.

Senator UDALL. We are getting about almost two-thirds through the list of members who are here to ask questions.

Senator Moran.

STATEMENT OF HON. JERRY MORAN,
U.S. SENATOR FROM KANSAS

Senator MORAN. Mr. Chairman, thank you.

Mr. Zuckerberg, I am over here. Thank you for your testimony and thank you for your presence here today.

On March 26 of this year, the FTC confirmed that it was investigating Facebook to determine whether its privacy practices violated the FTC Act or the Consent Order that Facebook entered into with the agency in 2011. I chair the Commerce Committee subcommittee that has jurisdiction over the Federal Trade Commission. I remain interested in Facebook's assertion that it rejects any suggestion of violating that Consent Order.

Part two of that Consent Order requires that Facebook, quote, "clearly and prominently display notice and obtain users' affirmative consent" before sharing their information with, quote, "any third party." My question is how does the case of approximately 87 million Facebook friends having their data shared with a third party due to the consent of only 300,000 consenting users not violate that agreement?

Mr. ZUCKERBERG. Well, Senator, like I said earlier, our view earlier is that we believe that we are in compliance with the Consent Order, but I think that we have a broader responsibility to protect people's privacy even beyond that. And in this specific case, the way that the platform worked or that you could sign into an app and bring some of your information and some of your friends' information is how we explained it would work. People had settings to that effect. We explained and they consented to it working that way. And the system basically worked as it was designed. The issue is that we designed the system in a way that was not good, and now starting in 2014, we have changed the design of the system so that way it just massively restricts the amount of data access that a developer can get.

Senator MORAN. The 300——

Mr. ZUCKERBERG. Going forward——

Senator MORAN.—I am sorry. The 300,000 people, they were treated in a way that was appropriate. They consented. But you are not suggesting that the friends consented?

Mr. ZUCKERBERG. Senator, I believe that we rolled out this developer platform and that we explained to people how it worked and that they did consent to it. It makes sense, I think, to go through the way the platform works. In 2007 we announced the Facebook developer platform, and the idea was that you wanted to make more experiences social, right? So, for example, you might want have a calendar that can have your friends' birthdays on it or you might want your address book to have your friends' pictures in it or you might want to map that and show your friends' addresses on it. In order to do that, we needed to build a tool that allowed people to sign into an app and bring some of their information and some of their friends' information to those apps. We made it very clear that this is how it worked, and when people signed up for Facebook, they signed up for that as well.

Now, a lot of good use cases came from that. I mean, there were games that were built, there were integrations with companies that I think we are familiar with like Netflix and Spotify. But over time,

what became clear was that that also enabled some abuse, and that is why in 2014 we took the step of changing the platforms, so now, when people sign into an appreciate, you do not bring some of your friends' information with you. You are only bringing your own information, and you are able to connect with friends who have also authorized that directly.

Senator MORAN. Let me turn to your bug bounty program. Our Subcommittee has had a hearing in regard to bug bounty. Your press release indicated that was one of the six changes that Facebook initially offered to crack down on platform abuses was to reward outside parties who find vulnerabilities. One concern I have regarding the utility of this approach is that the vulnerability disclosure programs are normally geared toward identifying unauthorized access to data, not pointing out data-sharing arrangement that likely could harm someone but technically abide by complex consent agreements. How do you see the bug bounty program that you have announced addressing the issue of that?

Mr. ZUCKERBERG. Sorry, could you clarify what specifically——

Senator MORAN. How do you see the bug bounty program that you have announced will deal with the sharing of information not permissible as compared to just unauthorized access to data?

Mr. ZUCKERBERG. Senator, I am not actually sure I understand this enough to speak to that specific point, and I can have my team follow up with you on the details of that.

[The information referred to follows:]

How can a bug bounty deal with reporting the sharing of data?

The Data Abuse Bounty Program, inspired by the existing Bug Bounty Program, helps us identify violations of our policies by requesting narrative descriptions of violations from individuals with direct and personal knowledge of events. The Data Abuse Bounty will reward people with first-hand knowledge and proof of cases where a Facebook platform app collects and transfers people's data to another party to be sold, stolen, or used for scams or political influence. We'll review all legitimate reports and respond as quickly as possible when we identify a credible threat to people's information. If we confirm data abuse, we will shut down the offending app and, if necessary, take legal action against the company selling or buying the data. We'll pay a bounty to the person who reported the issue or allow them to donate their bounty to a charity, and we'll also alert those we believe to be affected. We also encourage our users to report to us content that they find concerning or that results in a bad experience, as well as other content that may violate our policies. We review these reports and take action on abuse, like removing content and disabling accounts.

Mr. ZUCKERBERG. In general, bounty programs are an important part of the security arsenal for hardening a lot of systems. I think we should expect that we are going to invest a lot in hardening our systems ourselves and that we are going to audit and investigate a lot of the folks in our ecosystem. But even with that, having the ability to enlist other third parties outside of the company to be able to help us out by giving them an incentive to point out when they see issues I think is likely going to help us improve the security of the platform overall, which is why we did this.

Senator MORAN. Thank you, Mr. Zuckerberg.

Chairman THUNE. Thank you, Senator Moran.

Next up, Senator Booker.

STATEMENT OF HON. CORY BOOKER,
U.S. SENATOR FROM NEW JERSEY

Senator BOOKER. Thank you, Mr. Chairman.

Hello, Mr. Zuckerberg. As you know, much of my life has been focused on low-income communities, poor communities, working-class communities and trying to make sure that they have a fair shake. This country has a very bad history of discriminatory practices toward low-income Americans and Americans of color from the redlining, FHA practices, even from more recently really discriminatory practices in the mortgage business. I have always seen technology as a promise to democratize our nation, expand access, expand opportunities.

But unfortunately, we have also seen how platforms, technology platforms like Facebook can actually be used to double down on discrimination and give people more sophisticated tools with which to discriminate.

Now, in 2016, ProPublica revealed that advertisers could use ethnic affinity, a user's race, to market categories to potentially discriminate overall against Facebook users in the areas of housing, employment, and credit, echoing the dark history in this country and also in violation of Federal law. In 2016, Facebook committed to fixing this, that the advertisers who have access to this data to fixing it, but unfortunately, a year later, as ProPublica's article showed, they found that the system Facebook built was still allowing housing ads without applying—to go forward without applying these new restrictions that were put on.

Facebook then opted in a system that is very similar to what we have been talking about with Cambridge Analytica, that they could self-certify that they were not engaging in these practices and complying with Federal law using this self-certification, a way to overcome and to comply with rather Facebook's antidiscrimination policy.

Unfortunately, in a recent lawsuit, as of February 2018, alleges that discriminatory ads were still being created on Facebook, still disproportionally impacting low-income communities and communities of color. Given the fact that you allowed Cambridge Analytica to self-certify in a way that I think—at least I think you have expressed regret over, is self-certification the best and strongest way to safeguard against the misuse of your platform and protect the data of users and not let it be manipulated in such a discriminatory fashion?

Mr. ZUCKERBERG. Senator, this is a very important question, and, you know, in general, I think over time we are going to move toward more proactive review with more AI tools to help flag problematic content. In the near term, we have a lot of content on the platform, and it is hard to review every single thing up front. We do a quick screen. But I agree with you that I think in this specific case I am not happy with where we are, and I think it makes sense to really focus on making sure that these areas get more review sooner.

Senator BOOKER. And I know you understand that there is a growing distrust—I know a lot of civil rights organizations have met with you—about Facebook's sense of urgency to address these issues. There is a distrust that stems from the fact that I know—

I have had conversations with leaders on Facebook about the lack of diversity in the tech sector as well, people who are writing these algorithms, people who are actually policing for this data or policing for these problems. Are they going to be a part of a more diverse group that is looking at this? You are looking to hire, as you said, 5,000 new positions for, among other things, reviewing content, but we know in your industry the inclusivity, it is a real serious problem in your industry that lacks diversity in a very dramatic fashion. It is not just true with Facebook; it is true with the tech area as well.

And so it is very important for me to communicate that larger sense of urgency and what a lot of civil rights organizations are concerned with. And we should be working towards a more collaborative approach. And I am wondering if you would be open to opening your platform for civil rights organizations to really audit a lot of these companies dealing in areas of credit and housing to really audit what is actually happening and better have more transparency in working with your platform.

Mr. ZUCKERBERG. Senator, I think that is a very good idea, and I think we should follow up on the details of that.

Senator BOOKER. I also want to say that there was an investigation, something that is very disturbing to me is the fact that there have been law enforcement organizations that use Facebook's platform to surveille African-American organizations like Black Lives Matter. I know you have expressed support for the group—and Philando Castile's killing was a broadcast live on Facebook—but there are a lot of communities of color worried that the data could be used to surveille groups like Black Lives Matter, like folks who are trying to organize against substantive issues of discrimination in this country. Is this something that you are committed to addressing and to ensuring that the freedoms that civil rights activists and others are not targeted or their work not being undermined or people not using your platform to unfairly surveille and try to undermine the activities that those groups are doing?

Mr. ZUCKERBERG. Yes, Senator. I think that that is very important. We are committed to that. And, in general, unless law enforcement has a very clear subpoena or ability or reason to get access information, we are going to push back on that across the board.

Senator BOOKER. And then I would just like for the record because my time is expired, but there is a lawsuit against Facebook about discrimination, and you moved for the lawsuit to be dismissed because no harm was shown. Could you please submit to the record, if you believe that people of color were not recruited for various economic opportunities are being harmed, could you please clarify why you moved to dismiss the lawsuit for the record?

Chairman THUNE. For the record.

Senator BOOKER. Thank you.

[The information referred to follows:]

Would you open the Company to audit companies dealing in credit and housing?

Relman, Dane & Colfax, a respected civil rights law firm, will carry out a comprehensive civil rights assessment of Facebook's services and internal operations. Laura Murphy, a national civil liberties and civil rights leader, will help guide this process—getting feedback directly from civil rights groups, like The Leadership Con-

ference on Civil and Human Rights, and help advise Facebook on the best path forward.

And then for the record, my time has expired, but there's a lawsuit against Facebook about discrimination. You move for it to be dismissed because no harm was shown. Could you please submit to the record, you believe that people of color were not recruited for various economic opportunities or being harmed. Can you please clarify why you move to dismiss that lawsuit for the record?

We have Community Standards that prohibit hate speech, bullying, intimidation, and other kinds of harmful behavior. We hold advertisers to even stricter advertising policies to protect users from things like discriminatory ads. We don't want advertising to be used for hate or discrimination, and our policies reflect that. For example, we make it clear that advertisers may not discriminate against people based on personal attributes such as race, ethnicity, color, national origin, religion, age, sex, sexual orientation, gender identity, family status, disability, and medical or genetic condition. We educate advertisers on our anti-discrimination policy, and in some cases—including when we detect that an advertiser is running housing ads—we require advertisers to certify compliance with our anti-discrimination policy and anti-discrimination laws.

Chairman THUNE. Senator Heller is up next.

STATEMENT OF HON. DEAN HELLER,
U.S. SENATOR FROM NEVADA

Senator HELLER. All right, Mr. Chairman. Thank you. I appreciate the time, and thank you for being here. I am over here. Thanks. And thank you for taking time. I know it has been a long day, and I think you are at the final stretch here, but I am glad that you are here.

Yesterday, Facebook sent out a notification to 87 million users that information was given to Cambridge Analytica without their consent. My daughter was one of the 87 million, and six of my staff, all from Nevada, received this notification. Can you tell me how many Nevadans were among the 87 million that received this notification?

Mr. ZUCKERBERG. Senator, I do not have this broken out by state right now, but I can have my team follow up with you to get you the information.

Senator HELLER. OK. OK. I figured that would be the answer.

[The information referred to follows:]

Can you tell me how many Nevadans were among the 87 million that received this notification?

A state-by-state breakdown is available at *https://newsroom.fb.com/news/2018/04/restricting-data-access/*.

Senator HELLER. If, after going through this hearing and Nevadans no longer want to have a Facebook account, if that is the case, if a Facebook user deletes their account, do you delete their data?

Mr. ZUCKERBERG. Yes.

Senator HELLER. My kids have been on Facebook and Instagram for years. How long do you keep a user's data?

Mr. ZUCKERBERG. Sorry, can——

Senator HELLER. How long do you keep a user's data after they have left? If they choose to delete their account, how long do you keep their data?

Mr. ZUCKERBERG. I do not know the answer to that off the top of my head. I know we try to delete it as quickly as is reasonable. We have a lot of complex systems, and it takes a while to work

through all that, but I think we try to move as quickly as possible. And I can follow up or have my team follow up——

Senator HELLER. Yes.

Mr. ZUCKERBERG.—to get you the data on that.

Senator HELLER. OK.

[The information referred to follows:]

How long do you keep a user's data? How long do you keep a user's data once they have left? If they choose to delete their account, how long do you keep their data?

In general, when a user deletes their account, we delete things they have posted, such as their photos and status updates, and they won't be able to recover that information later. (Information that others have shared about them isn't part of their account and won't be deleted.)

There are some limited exceptions to these policies: For instance, information can be accessed and preserved for an extended period when it is the subject of a legal request or obligation, governmental investigation, or investigations of possible violations of our terms or policies, or otherwise to prevent harm. We also retain information from accounts disabled for terms violations for at least a year to prevent repeat abuse or other term violations.

Senator HELLER. Have you ever said that you will not sell an ad based on personal information, simply that you would not sell this data because of the usage of it goes too far?

Mr. ZUCKERBERG. Senator, could you clarify that?

Senator HELLER. Have you ever drawn the line on selling data to an advertiser?

Mr. ZUCKERBERG. Yes, Senator. We do not sell data at all. So the way that ad system works is advertisers can come to us and say I have a message that I am trying to reach a certain type of people. They might be interested in something, they might live in a place, and then we help them get that message in front of people. But this is one of the—it is widely mischaracterized about our system that we sell data, and it is actually one of the most important points of how Facebook works is we do not sell data. Advertisers do not get access to people's individual data.

Senator HELLER. Have you ever collected the content of phone calls or messages through any Facebook application or service?

Mr. ZUCKERBERG. Senator, I do not believe we have ever collected the content of phone calls. We have an app called Messenger that allows people to message mostly their Facebook friends, and we do, on the android operating system, allow people to use that app as their client for both Facebook messages and texts, so we do allow people to import their texts into that.

Senator HELLER. OK. Let me ask you about government surveillance. For years, Facebook said that there should be strict limits on the information the government can access on Americans. And, by the way, I agreed with you because privacy is important to Nevadans. You argue that Facebook users would not trust you if they thought you were giving their private information to the intelligence community, yet you use and sell the same data to make money. And in the case of Cambridge Analytica, you do not even know how it is used after you sell it. Can you tell us why this is not hypocritical?

Mr. ZUCKERBERG. Well, Senator, once again, we do not sell any data to anyone. We do not sell it to advertisers, and we do not sell it to developers. What we do allow is for people to sign in to apps

and bring their data—and it used to be the date of some of their friends, but now it is not—with them. And that I think makes sense. I mean, that is basic data portability, the ability that you own the data; you should be able to take it from one app to another if you would like.

Senator HELLER. Do you believe you are more responsible with millions of Americans' personal data than the Federal Government would be?

Mr. ZUCKERBERG. Yes. But, Senator, your point about surveillance, I think that there is a very important distinction to draw here, which is that when organizations do surveillance, people do not have control over that, right? On Facebook, everything that you share there you have control over. You can say I do not want this information to be there. You have full access to understand every piece of information that Facebook might know about you, and you can get rid of all of it. And I do not know of any surveillance organization in the world that operates that way, which is why I think that that comparison just is not really apt here.

Senator HELLER. With you here today, do you think you are a victim?

Mr. ZUCKERBERG. No.

Senator HELLER. Do you think Facebook as a company is a victim?

Mr. ZUCKERBERG. Senator, no. I think we have a responsibility to protect everyone in our community from anyone in our ecosystem who is going to potentially harm them.

And I think that we have not done enough historically and we need to step up and do more.

Senator HELLER. Do you consider the 87 million users, do you consider them victims?

Mr. ZUCKERBERG. Senator, I think yes. I mean, they did not want their information to be sold to Cambridge Analytica by a developer, and that happened, and it happened on our watch, so even though we did not do it, I think we have a responsibility to be able to prevent that and be able to take action sooner. And we are committing to make sure that we do that going forward, which is why the steps that I announced before are now—the two most important things that we are doing are locking down the platform to make sure that developers cannot get access to that much data so this cannot happen again going forward, which I think is largely the case since 2014, and, going backwards, we need to investigate every single app that might have had access to a large amount of people's data to make sure that no one else was misusing it. And if we find that they are, we are going to get into their systems, do a full audit, make sure they delete it, and we are going to tell everyone who is affected.

Senator HELLER. Mr. Chairman, thank you.

Chairman THUNE. Thank you, Senator Heller.

We will go to Senator Peters and then into the break and then Senator Tillis coming out of the break, so, Senator Peters.

STATEMENT OF HON. GARY PETERS,
U.S. SENATOR FROM MICHIGAN

Senator PETERS. Thank you, Mr. Chairman.

Mr. Zuckerberg, thank you for being here today.

You know, you have talked about your very humble beginnings in starting Facebook in your dorm room, which I appreciated that story, but certainly, Facebook has changed an awful lot over a relatively short period of time. When Facebook launched its timeline feature, consumers saw their friends post chronologically was the process. Facebook has since then changed to a timeline driven by some very sophisticated logarithms, and I think it has left many people as a result of that asking, you know, why am I seeing this feed, and why am I seeing this right now?

And now, in light of the Cambridge Analytica issue, Facebook users are asking I think some new questions right now. Can I believe what I am seeing, and who has access to this information about me? So I think it is safe to say very simply that Facebook is losing the trust of an awful lot of Americans as a result of this incident.

And I think an example of this is something that I have been hearing a lot from folks who have been coming up to me and talking about really kind of an experience they have had where they are having a conversation with friends, not on the phone just talking, and then they see ads popping up fairly quickly on their Facebook. So I have heard constituents here that Facebook is mining audio from their mobile devices for the purpose of ad targeting, which I think speaks to this lack of trust that we are seeing here. And I understand there are some technical issues and logistical issues for that to happen, but for the record, I think it is clear, seeing I hear it all the time, including for my own staff, yes or no, does Facebook use audio obtained from mobile devices to enrich personal information about its users?

Mr. ZUCKERBERG. No.

Senator PETERS. OK. The——

Mr. ZUCKERBERG. Well, Senator, let me be clear on this. So you are talking about this conspiracy theory that gets passed around that we listen to what is going on on your microphone and use that for ads?

Senator PETERS. Right.

Mr. ZUCKERBERG. We do not do that. To be clear, we do allow people to take videos on their devices and share those, and of course videos also have audio, so we do, while you are taking a video, record that and use that to make the service better by making sure that your videos have audio but, I mean, that I think it is pretty clear, but I just wanted to make sure I was exhaustive there.

Senator PETERS. Well, I appreciate that. And hopefully, that will dispel a lot of what I have been hearing, so thank you for saying that.

Certainly, today, in the era of mega-data, we are finding that data drives everything, including consumer behaviors. And consumer information is probably the most valuable information you can get in the data ecosystem. And certainly folks, as you have mentioned in your testimony here, people like the fact that they can have targeted ads that they are going to be interested in as opposed to being bombarded by a lot of ads that they do not have any interest in, and that consumer information is important in order

for you to tailor that. But also, people are now beginning to wonder is there an expense to that when it comes to perhaps exposing them to being manipulated or through deception.

You have talked about artificial intelligence. You brought that up many times during your testimony, and I know you have employed some new algorithms to target bots, bring down fake accounts, deal with terrorism, things that you have talked about in this hearing. But you also know that artificial intelligence is not without its risks and that you have to be very transparent about how those algorithms are constructed. How do you see artificial intelligence more specifically dealing with the ecosystem by helping to get consumer insights but also keeping consumer privacy safe?

Mr. ZUCKERBERG. Senator, I think the core question you are asking about AI transparency is a really important one that people are just starting to very seriously study, and that is ramping up a lot. And I think this is going to be a very central question for how we think about AI systems over the next decade and beyond.

Right now, a lot of our AI systems make decisions in ways that people do not really understand.

Senator PETERS. Right.

Mr. ZUCKERBERG. And I do not think that in 10 or 20 years in the future that we all want to build we want to end up with systems that people do not understand how they are making decisions. So doing the research now to make sure that these systems can have those principles as we are developing them I think is certainly an extremely important thing.

Senator PETERS. Well, you bring up the principles because, as you are well aware, AI systems, especially in very complex environments when you have machine learning, it is sometimes very difficult to understand, as you mentioned, exactly how those decisions were arrived at. There are examples of how decisions are made on a discriminatory basis and that they can compound if you are not very careful about how that occurs. And so is your company—you mentioned principles. Is your company developing a set of principles that are going to guide that development? And would you provide details to us as to what those principles are and how they will help deal with this issue?

Mr. ZUCKERBERG. Yes, Senator. I can make sure that our team follows up and gets you the information on that.

[The information referred to follows:]

Well, you bring up the principles because, as you are well aware, AI systems, especially in very complex environments when you have machine learning, it is sometimes very difficult to understand, as you mentioned, exactly how those decisions were arrived at. There are examples of how decisions are made on a discriminatory basis and that they can compound if you are not very careful about how that occurs. And so is your company—you mentioned principles. Is your company developing a set of principles that are going to guide that development? And would you provide details to us as to what those principles are and how they will help deal with this issue?

We are focused on both the technical and the ethical aspects of artificial intelligence. We believe these two should go hand-in-hand together in order to fulfill our commitment to being fair, transparent, and accountable in our development and use of AI. Facebook has AI teams working on developing the philosophical, as well as technical, foundations for this work. Facebook is also one of the co-founders and members of the Partnership on AI (PAI), a collaborative and multi-stakeholder organization established to study and formulate best practices on AI technologies, to advance the public's understanding of AI, and to serve as an open platform for discus-

sion and engagement about AI and its influences on people and society. The thematic pillars that structure the work we're doing in the scope of the PAI—safety, fairness, transparency, and accountability—are the principles that we believe industry should follow and promote when building and deploying AI systems. The PAI's Fair, Transparent and Accountable AI Working Group is also working alongside industry, academia, and civil society to develop best practices around the development and fielding of fair, explainable, and accountable AI systems.

Mr. ZUCKERBERG. And we have a whole AI ethics team that is working on developing basically the technology. It is not just about philosophical principles; it is also a technological foundation for making sure that this goes in the direction that we want.

Senator PETERS. Thank you.

Chairman THUNE. Thank you, Senator Peters. We will recess for five and come back in, so we will give Mr. Zuckerberg a quick break here. Thanks.

[Recess.]

Chairman THUNE. All right. We are at that final stretch. And Senator Tillis is recognized.

STATEMENT OF HON. THOM TILLIS,
U.S. SENATOR FROM NORTH CAROLINA

Senator TILLIS. Thank you, Mr. Zuckerberg, for being here. I think you have done a good job. I have been here for most of the session except for about 20 minutes I watched on television back in my office.

I was Googling earlier, actually going on my Facebook app on my phone earlier, and I found one of your Facebook—or, yes, one of your Facebook presences. It was the same one on March 30. I think you posted a pic of a First Seder, but further down, you listed out the facts since the new platform was released in 2007, sort of a timeline. You start with 2007 and then you jump to the Cambridge Analytica issue. I actually think that we need to fully examine what Cambridge Analytica did. They either broke a kind of code of conduct. If they broke any other rules or agreements with you all, I hope that they suffer the consequences.

But I think that timeline needs to be updated, and it really needs to go back—I have read a series of three articles that were published in the *MIT Technology Review* back in 2012, and it talks about how proud the Obama campaign was of exploiting data on Facebook in the 2012 campaign. In fact, somebody asked you earlier if it made you mad about what Cambridge Analytica did, and you rightfully answered yes, but I think you should probably be equally mad when a former campaign director of the Obama campaign proudly tweeted, "Facebook was surprised we were able to suck out the whole social graph, but they did not stop us once they realized that was what we were doing." So you clearly had some people in your employ that apparently knew it. At least that is what this person said on Twitter, and thank goodness for Wayback and some of the other history-grabber machines. I am sure we can get this tweet back and get it in the right context.

I think when you do your research, it is important to get the whole view. I worked in data analytics practice for a good part of my career, and for anybody to pretend that Cambridge Analytica was the first person to exploit data clearly does not work or has not worked in the data analytics field. So when you go back and

do your research on Cambridge Analytica, I would personally appreciate it if you would start back from the first known high-profile national campaign that exploited Facebook data. In fact, they published an app that said it would grab information about my friends, their birth dates, locations, and likes.

So presumably, if I downloaded that app that was published by the Obama campaign—I have got 4,900 friends on my Facebook page; I delete the haters and save room for family members and true friends on my personal page, as I am sure everybody does—then that means if I clicked yes on that app, I would have approved the access of birth dates, locations, and likes of some 4,900 people without their consent.

So as you do the chronology, I think it would be very helpful so that we can take away the partisan rhetoric that is going on like this is a Republican-only issue. It is a broad-based issue that needs to be fixed. And bad actors at either end of the political spectrum need to be held accountable, and I trust that you all are going to work on that.

I think the one thing that I—so, for that, I just want to get to the facts, and there is no way you could answer any of the questions, so I am not going to burden you with that. But I think, given that chronology, it would be very helpful.

The one thing I would encourage people to do is go to Facebook—I am a proud member of Facebook. I just got a post from my sister on this being National Sibling Day, so I have connected with four or five of my staff while I was giving you my undivided—or family undivided attention. But go to the privacy tab. If you do not want to share something, do not share it. This is a free service. Go on there and say I do not want to allow third-party search engines to get in my Facebook page. Go on there and say only my friends can look at it. Go in there and understand what you are signing up for. It is a free app.

Now, you need to do more, and I think it would be helpful. I did not read your disclaimer page or the terms of use because I did not see anywhere in there that I could get an attorney and negotiate the terms, so it was a terms of use. I went on there, then I used the privacy settings to be as safe as I could be with a presence on Facebook.

Last thing, we talk about all these proposed legislation, good ideas, but I have one question for you. When you were developing this app in your dorm, how many people did you have in your regulatory affairs division?

[Laughter.]

Senator TILLIS. Exactly. So if government takes a heavy-handed approach to fix this problem, then we know very well that the next Facebook, the next thing that you are going to wake up and worry about how you continue to be relevant as the behemoth that you are today is probably not going to happen. So I think that there is probably a place for some regulatory guidance here, but there is a huge place for Google, Snapchat, Twitter, all the other social media platforms to get together and create standards.

And I also believe that that person who may have looked the other way when the whole social graph was extracted for the Obama campaign, if they are still working for you, they probably

should not or at least there should be a business code of conduct that says you do not play favorites. You are trying to create a fair place for people to share their ideas.

Thank you for being here.

Chairman THUNE. Thank you, Senator Tillis.

Senator Harris.

STATEMENT OF HON. KAMALA HARRIS,
U.S. SENATOR FROM CALIFORNIA

Senator HARRIS. Thank you. Thank you for being here.

I have been here on and off for the last 4 hours that you have been testifying, and I have to tell you that I am concerned about how much Facebook values trust and transparency if we agree that a critical component of a relationship of trust and transparency is we speak truth and we get to the truth.

During the course of this hearing these last four hours, you have been asked several critical questions for which you do not have answers, and those questions have included whether Facebook can track users' browsing activity even after the user has logged off of Facebook, whether Facebook can track your activity across devices even when you are not logged into Facebook, who is Facebook's biggest competition, whether Facebook may store up to 96 categories of users' information, whether you knew Kogan's terms of service and whether you knew that Kogan could sell or transfer data.

And then another case in point specifically as it relates to Cambridge Analytica, and a concern of mine, is that you, meaning Facebook—and I am going to assume you personally as CEO became aware in December 2015 that Dr. Kogan and Cambridge Analytica misappropriated data from 87 million Facebook users. That is 27 months ago that you became, as Facebook, and perhaps you personally became aware. However, a decision was made not to notify the users.

So my question is, did anyone at Facebook have a conversation at the time that you became aware of this breach—and have a conversation wherein the decision was made not to contact the users?

Mr. ZUCKERBERG. Senator, I do not know if there were any conversations at Facebook overall because I was not in a lot of them, but——

Senator HARRIS. On that subject?

Mr. ZUCKERBERG. Yes. I mean, I am not sure what other people discussed. In 2015 we heard the report that this developer Aleksandr Kogan had sold data to Cambridge Analytica.

Senator HARRIS. And were——

Mr. ZUCKERBERG. That is in violation of our terms.

Senator HARRIS. Correct. And were you a part of a discussion that resulted in a decision not to inform your users?

Mr. ZUCKERBERG. I do not remember a conversation like that for the reason why——

Senator HARRIS. Are you aware of anyone in leadership at Facebook who was in a conversation where a decision was made not to inform your users, or do you believe no such conversation ever took place?

Mr. ZUCKERBERG. I am not sure whether there was a conversation about that, but I can tell you the thought process at the time

of the company, which was that in 2015 when we heard about this, we banned the developer and we demanded that they delete all the data and stop using it, and the same with Cambridge Analytica.

Senator HARRIS. And I appreciate your——

Mr. ZUCKERBERG. They told us they had——

Senator HARRIS.—your testimony in that regard, but I am talking about notification of the users, and this relates to the issue of transparency and the relationship of trust, informing the user about what you know in terms of how their personal information has been misused. And I am also concerned that when you personally became aware of this, did you or senior leadership do an inquiry to find out who at Facebook had this information, and did they not have a discussion about whether or not the users should be informed back in December 2015?

Mr. ZUCKERBERG. Senator, in retrospect, I think we clearly view it as a mistake that we did not inform people, and we did that based on false information that we thought that the case was closed and that the data had been deleted.

Senator HARRIS. So there was a decision made on that basis not to inform the users, is that correct?

Mr. ZUCKERBERG. That is my understanding, yes.

Senator HARRIS. OK. And——

Mr. ZUCKERBERG. But, in retrospect, I think that was a mistake, and knowing what we know now, we should have handled a lot of things here differently.

Senator HARRIS. And I appreciate that point. Do you know when that decision was made not to inform the users?

Mr. ZUCKERBERG. I do not.

Senator HARRIS. OK. Last November, the Senate Intelligence Committee held a hearing on social media influence. I was a part of that hearing. I submitted 50 written questions to Facebook and other companies, and the responses that we received were unfortunately evasive and some are frankly nonresponsive. So I am going to ask the question again here. How much revenue did Facebook earn from the user engagement that resulted from foreign propaganda?

Mr. ZUCKERBERG. Well, Senator, what we do know is that the IRA, the Internet Research Agency, the Russian firm, ran about $100,000 worth of ads.

Senator HARRIS. How much did Facebook——

Mr. ZUCKERBERG. I cannot say that we have identified all of the foreign actors who were involved here, so I cannot say that that is all of the money, but that is what we have identified.

Senator HARRIS. OK. My time is up. I will submit more questions for the record. Thank you.

Chairman THUNE. Thank you, Senator Harris.

Next up is Senator Kennedy.

STATEMENT OF HON. JOHN KENNEDY,
U.S. SENATOR FROM LOUISIANA

Senator KENNEDY. Mr. Zuckerberg, I come in peace.

[Laughter.]

Senator KENNEDY. I do not want to have to vote to regulate Facebook, but, by God, I will. A lot of that depends on you. I am

a little disappointed in this hearing today. I just do not feel like that we are connecting. So let me try to lay it out for you from my point of view. I think you are a really smart guy, and I think you have built an extraordinary American company, and you have done a lot of good. Some of the things that you have been able to do are magical. But our promised digital utopia we have discovered has minefields. There are some impurities in the Facebook punch bowl, and they have got to be fixed. And I think you can fix them.

Now, here is what is going to happen. There are going to be a whole bunch of bills introduced to regulate Facebook. It is up to you whether they pass or not. You can go back home, spend $10 million on lobbyists and fight us, or you can go back home and help us solve this problem. And there are two. One is a privacy problem; the other one is what I call a propaganda problem. Let us start with the privacy problem first. Let us start with the user agreement.

Here is what everybody has been trying to tell you today, and I say this gently. Your user agreement sucks.

[Laughter.]

Senator KENNEDY. You can spot me 75 IQ points. If I can figure it out, you can figure it out. The purpose of that user agreement is to cover Facebook's rear end. It is not to inform your users about their rights. Now, you know that and I know that. I am going to suggest to you that you go back home and rewrite it and tell your $1,200-an-hour lawyers—no disrespect; they are good—but tell them you want it written in English and non-Swahili so the average American can understand it. That would be a start.

As a Facebook user, are you willing to give me more control over my data?

Mr. ZUCKERBERG. Senator, as someone who uses Facebook, I believe that you should have complete control over your data.

Senator KENNEDY. OK. Are you willing to go back and work on giving me a greater right to erase my data?

Mr. ZUCKERBERG. Senator, you can already delete any of the data that is there or delete all of your data.

Senator KENNEDY. Are you willing to work on expanding that?

Mr. ZUCKERBERG. Senator, I think we already do what you are referring to, but certainly, we are always working on trying to make these controls easier.

Senator KENNEDY. Are you willing to expand my right to know who you are sharing my data with?

Mr. ZUCKERBERG. Senator, we already give you a list of apps that you are using, and you sign into those yourself and provide affirmative consent.

Senator KENNEDY. Right, on that——

Mr. ZUCKERBERG. And as I have said before, we do not share any data with——

Senator KENNEDY.—user agreement. Are you willing to expand my right to prohibit you from sharing my data?

Mr. ZUCKERBERG. Senator, again, I believe that you already have that control, so, I mean, I think people have that full control in the system already today. If we are not communicating this clearly, then that is a big thing that we should work on because I think

the principles that you are articulating are the ones that we believe in and try to codify in the product that we build.

Senator KENNEDY. Are you willing to give me the right to take my data on Facebook and move it to another social media platform?

Mr. ZUCKERBERG. Senator, you can already do that. We have a download-your-information tool where you can go, get a file of all the content there, and then do whatever you want with it.

Senator KENNEDY. Then I assume you are willing to give me the right to say I am going to go on your platform and you are going to be able to tell a lot about me as a result, but I do not want you to share it with anybody?

Mr. ZUCKERBERG. Yes, Senator, and I believe you already have that ability today. People can sign on and choose to not share things and just follow some friends or some pages and read content if that is what they want to do.

Senator KENNEDY. OK. I want to be sure—I am about out of time. Boy, it goes fast, does it not? Let me ask you one final question in my 12 seconds. Could somebody call you up and say I want to see John Kennedy's file?

Mr. ZUCKERBERG. Absolutely not.

Senator KENNEDY. Not would you do it, could you do it?

Mr. ZUCKERBERG. In theory——

Senator KENNEDY. Do you have the right to put my data, a name on my data, and share it with somebody?

Mr. ZUCKERBERG. I do not believe we have the right to do that.

Senator KENNEDY. Do you have the ability?

Mr. ZUCKERBERG. Senator, the data is in the system, so——

Senator KENNEDY. Do you have the ability?

Mr. ZUCKERBERG. Technically, I think someone could do that, but that would be a massive breach, so we would never do that.

Senator KENNEDY. It would be a breach. Thank you, Mr. Chairman.

Chairman THUNE. Thank you, Senator Kennedy.

Senator Baldwin is up next.

STATEMENT OF HON. TAMMY BALDWIN,
U.S. SENATOR FROM WISCONSIN

Senator BALDWIN. Thank you, Mr. Chairman.

Thank you for being here and enduring the long day, Mr. Zuckerberg.

I want to start with what I hope can be a quick round of questions just so I make sure I understand your previous testimony.

Specifically with regard to the process by which Cambridge Analytica was able to purchase Facebook users' data, so it was an app developer Aleksandr Kogan, he collected data via a personality quiz. Is that correct?

Mr. ZUCKERBERG. Yes.

Senator BALDWIN. OK. And he thereby is able to gain access of not only the people who took the quiz but their network? Is that correct, too?

Mr. ZUCKERBERG. Senator, yes. The terms of the platform at the time allowed for people to share their information and some basic information about their friends as well. And we have since changed that. As of 2014——

Senator BALDWIN. And——

Mr. ZUCKERBERG.—now, that is not possible.

Senator BALDWIN. And so, in total, about 87 million Facebook users. You earlier testified about the two types of ways you gain data. One is what is voluntarily shared by Facebook members and users, and the other is in order to I think you said improve your advertising experience, whatever that exactly means, the data that Facebook collects in order to customize or focus on that. Was Aleksandr Kogan able to get both of those sets of data or just what was voluntarily entered by the user?

Mr. ZUCKERBERG. Yes, that is a good question. It was just a subset of what was entered by the person. And——

Senator BALDWIN. So a subset of the 95 categories of data that you keep?

Mr. ZUCKERBERG. Yes, when you sign into an app——

Senator BALDWIN. OK.

Mr. ZUCKERBERG.—the app developer has to say here are the types of data from you that I am asking for, including public information like your name and profile, the pages you follow, other interests on your profile, that kind of content.

Senator BALDWIN. OK.

Mr. ZUCKERBERG. The app developer has to disclose that upfront and you agree to it.

Senator BALDWIN. OK. So in answer to a couple of other Senators' questions, specifically Senator Fischer, you talked about Facebook storing this data and I think you just talked about the data being in the system. I wonder if outside of the way in which Aleksandr Kogan was able to access this data, whether you—could Facebook be vulnerable to a data breach or hack? Why or why not?

Mr. ZUCKERBERG. Well, there are many kinds of security threats that a company like ours faces, including people trying to break into our security systems——

Senator BALDWIN. OK. And if you believe that you had been hacked, do you believe you would have the duty to inform those who were impacted?

Mr. ZUCKERBERG. Yes.

Senator BALDWIN. OK. Do you know whether Aleksandr Kogan sold any of the data he collected with anyone other than Cambridge Analytica?

Mr. ZUCKERBERG. Senator, yes, we do. He sold it to a couple of other firms.

Senator BALDWIN. Can you identify them?

Mr. ZUCKERBERG. Yes, there is one called Eunoia, and there may have been a couple of others as well, and I can follow up with you——

Senator BALDWIN. Can you furnish that to me after?

Mr. ZUCKERBERG. Yes.

[The information referred to follows:]

Do you know whether Aleksandr Kogan sold any of the data he collected to anyone other than Cambridge Analytica?

Kogan represented to us that he provided data to SCL, Eunoia Technologies (a company founded by Christopher Wylie), and a researcher at the Toronto Laboratory for Social Neuroscience at the University of Toronto. He represented to Facebook that he only received payment from SCL/Cambridge Analytica.

Senator BALDWIN. Thank you. I appreciate that. And then how much do you know or have you tried to find out how Cambridge Analytica used the data while they had it before you believe they deleted it?

Mr. ZUCKERBERG. Since we just heard that they did not delete it about a month ago, we have kicked off an internal investigation to see if they used that data in any of their ads, for example. That investigation is still underway, and we can come back to you with the results of that once we have that.

[The information referred to follows:]

How much do you know or have you tried to find out how Cambridge Analytica used the data while they had it before you believed they deleted it?

On December 11, 2015, *The Guardian* published an article reporting that Kogan and his company, GSR, may have passed information his app had obtained from Facebook users to SCL Elections Ltd. (SCL)/Cambridge Analytica. By doing so, Kogan and his company violated Facebook's Platform Policies, which explicitly prohibited selling or licensing user data accessed from Facebook and from sharing any user data accessed from Facebook with any ad network, data broker or other advertising or monetization-related service. For this reason, Facebook immediately banned his app from our platform and launched an investigation into these allegations. Kogan signed a certification declaring that he had deleted all data that he obtained through his app and obtained certifications of deletion from others he had shared data with, including Cambridge Analytica. In March 2018, new allegations surfaced that Cambridge Analytica may not have deleted data as it had represented. Our investigation of these matters is ongoing.

Senator BALDWIN. OK. I want to switch to my home State of Wisconsin. According to press reports, my home State of Wisconsin was a major target of Russian-bought ads on Facebook in the 2016 election. These divisive ads touching on a number of very polarizing issues were designed to interfere with our election.

We have also learned that Russian actors using another platform Twitter similarly targeted Wisconsin with divisive content aimed at sowing division and dissent, including in the wake of a police-involved shooting in Milwaukee's Sherman Park neighborhood in August 2016.

Now, I find some encouragement in the steps you have outlined today to provide greater transparency regarding political ads. I do want to get further information on how you can be confident that you have excluded entities based outside of the United States.

Mr. ZUCKERBERG. We will follow up on that.

[The information referred to follows:]

I find some encouragement in the steps you have outlined today to provide greater transparency regarding political ads. I want to get further information on how you can be confident that you have excluded entities based outside of the United States.

Pursuant to the new transparency measures Facebook is launching, all advertisers who want to run ads with political content targeted at the U.S. will have to confirm their identity and location by providing either a U.S. driver's license or passport, last four digits of their social security number, and a residential mailing address. In addition, people who manage Pages with large numbers of followers will need to be verified. Those who manage large Pages that do not clear the process will no longer be able to post.

Senator BALDWIN. And then I think on that topic, if you require disclosure of a political ad's sponsor, what sort of transparency will you be able to provide with regard to people who were not the subject of that ad seeing its content?

Mr. ZUCKERBERG. Senator, you will be able to go to any page and see all of the ads that that page has run, so if someone is running

a political campaign, for example, and they are targeting one district with one ad and another district with another, historically, it has been hard to track that down, but now, it will be very easy. You will just be able to look at all of the ads that they have run, the targeting associated with each to see what they are saying to different folks and in some cases how much they are spending on the ads and all of the relevant information. This is an area where I think more transparency will really help discourse overall and root out foreign interference in elections.

Senator BALDWIN. And will you——

Chairman THUNE. Thank you, Senator Baldwin.

Senator Johnson.

STATEMENT OF HON. RON JOHNSON,
U.S. SENATOR FROM WISCONSIN

Senator JOHNSON. Thank you, Mr. Chairman.

Thank you, Mr. Zuckerberg, for testifying here today. Do you have any idea how many of your users actually read the terms of service, the privacy policy, the statement of rights and responsibilities, I mean, actually read it?

Mr. ZUCKERBERG. Senator, I do not.

Senator JOHNSON. Would you imagine it is a very small percentage?

Mr. ZUCKERBERG. Senator, who read the whole thing? I would imagine that probably most people do not read the whole thing, but everyone has the opportunity to and consents to it.

Senator JOHNSON. Well, I agree, but that is kind of true of every application where, you know, you want to get to it, and you have to agree to it and people just press that agree, the vast majority, correct?

Mr. ZUCKERBERG. Senator, it is really hard for me to make a full assessment, but——

Senator JOHNSON. Common sense will tell you that would be probably the case.

With all this publicity, have you documented any kind of backlash from Facebook users? I mean, has there been a dramatic falloff in the number of people who utilize Facebook because of these concerns?

Mr. ZUCKERBERG. Senator, there has not.

Senator JOHNSON. Do you have any witness to any?

Mr. ZUCKERBERG. Senator, there was a movement where some people were encouraging their friends to delete their account, and I think that that got shared a bunch.

Senator JOHNSON. So it is kind of safe to say that Facebook users don't seem to be overly concerned about all these revelations, although obviously Congress apparently is?

Mr. ZUCKERBERG. Well, Senator, I think people are concerned about it, and I think these are incredibly important issues that people want us to address. And I think people have told us that very clearly.

Senator JOHNSON. So it seems like Facebook users still want to use the platform because they enjoy sharing photos and they share the connectivity with the family members, that type of thing, and that overrides their concerns about privacy.

You talk about the user owns the data. You know, there have been a number of proposals of having that data stay at the user and allow the user to monetize it themselves. Your COO Ms. Sandberg mentioned possibly if you can't utilize that data to sell advertising, perhaps we would charge people to go into Facebook. Have you thought about that model where the user data is actually monetized by the actual user?

Mr. ZUCKERBERG. Senator, I am not sure exactly how it would work for it to be monetized by the person directly. In general, we believe that the ads model is the right one for us because it aligns with our social mission of trying to connect everyone and bring the world close together.

Senator JOHNSON. But you are aware of people making that kind of proposal, correct?

Mr. ZUCKERBERG. Yes, Senator, a number of people suggest that we should offer a version where people cannot have ads if they pay a monthly subscription, and certainly we consider ideas like that. I think that they are reasonable ideas to think through. But overall, I think that the ads experience is going to be the best one. I think in general people like not having to pay for a service. A lot of people can't afford to pay for a service around the world. And this aligns with our mission the best.

Senator JOHNSON. You answered Senator Graham when he asked you if you thought you were a monopoly that you didn't think so. You are obviously a big player in this space. That might be an area for competition, correct, if somebody else wants to create a social platform that allows a user to monetize their own data?

Mr. ZUCKERBERG. Senator, yes. There are lots of new social apps all the time, and as I said before, the average American I think uses eight different communication and social apps, so there is a lot of different choice and a lot of innovation and activity going on in this space.

Senator JOHNSON. I want to, in a very short period of time, for you to talk about the difference between advertisers and application developers because those, again, you said in earlier testimony that advertisers have no access to data whatsoever, but application developers do. Now, is that only through their own service agreements with their customers, or do they actually access data as they are developing applications?

Mr. ZUCKERBERG. Senator, this is an important distinction, so thanks for giving me the opportunity to clarify this. We give people the ability to take their data to another app if they want. Now, this is a question that Senator Kennedy asked me just a few minutes ago. The reason why we designed the platform that way is because we thought it would be very useful to make it so that people could easily bring their data to other services. Some people in the company argued against that at the time because they were worried that—they said, hey, we should just make it so that we can be the only ones who develop this stuff and we thought that that was a useful thing for people to do so we built it.

Senator JOHNSON. That is the user agreeing to allow you to share when they are using that app to allow Facebook to share their data. Does the developer ever have access to that prior to users using it? I mean, in developing the application because you used

the term scraped data. What does that mean? Who scraped the data?

Mr. ZUCKERBERG. Yes, Senator, this is a good question. So there is the developer platform, which is the sanctioned way that an app developer can ask a person to access information. We also have certain features and certain things that are public, right? A lot of the information that people choose to put on Facebook they are sharing with everyone in the world, not privately but, you know, you put your name, you put your profile picture. That is public information that people put out there. And sometimes people who aren't registered developers at Facebook try to load a lot of pages in order to get access to a bunch of people's public information and aggregate it. We fight back hard against that because we do not want anyone to aggregate information even if people made it public and chose to share it with everyone.

Senator JOHNSON. OK. Thank you, Mr. Chairman.

Chairman THUNE. Thank you, Senator Johnson.

Senator Hassan.

STATEMENT OF HON. MAGGIE HASSAN,
U.S. SENATOR FROM NEW HAMPSHIRE

Senator HASSAN. Thank you, Mr. Chair.

Thank you, Mr. Zuckerberg, for being here today.

I want to talk to a couple of broader issues. I am concerned that Facebook's profitability rests on two potentially problematic foundations, and we have heard other Senators talk about this a little today. The foundations are maximizing the amount of time people spend on your products and collecting people's data. I have looked at Facebook's 2017 corporate financial statement where you lay out some of the major risks to your business. One risk is a decrease in, and I quote, "user engagement, including time spent on our products." That concerns me because of the research we have seen suggesting that too much time spent on social media can hurt people's mental health, especially young people.

Another major risk to your business is a potential decline in—and here is another quote—"the effectiveness of our ad targeting or the degree to which users opt out of certain types of ad targeting, including as a result of changes that enhance the user's privacy." There is clearly tension, as other Senators have pointed out, between your bottom line and what is best for your users.

You have said in your testimony that Facebook's mission is to bring the world closer together, and you have said that you will never prioritize advertisers over that mission. And I believe that you believe that. But at the end of the day, your business model does prioritize advertisers over the mission. Facebook is a for-profit company, and as the CEO, you have a legal duty to do what is best for your shareholders.

So given all of that, why should we think that Facebook on its own will ever truly be able to make the changes that we need it to make to protect Americans' well-being and privacy?

Mr. ZUCKERBERG. Well, Senator, you raise a number of important points in there, so let me respond——

Senator HASSAN. Sure.

Mr. ZUCKERBERG.—in a couple of different ways. The first is that I think it is really important to think about what we are doing is building this community over the long term. Any business has the opportunity to do things that might increase revenue in the short term but at the expense of trust or building engagement over time. What we actually find is not necessarily that increasing time spent, especially not just in the short term, is going to be best for our business. It actually aligns very closely with the well-being research that we have done, that when people are interacting with other people and posting and basically building relationships, that is both correlated with higher measures of well-being, health, happiness, not feeling lonely, and that ends up being better for the business than when they are doing lower-value things like just passively consuming content. So I think that that is an important point to——

Senator HASSAN. OK. And I understand the point that you are trying to make here, but here is what I am concerned about. We have heard this point from you over the last decade-plus since you founded Facebook, and I understand that you founded it pretty much as a solo entrepreneur with your roommate, but now, you know, you are sitting here, the head of a bazillion-dollar company. And we have heard you apologize numerous times and promise to change, but here we are again, right?

So I really firmly believe in free enterprise, but when private companies are unwilling or unable to do what is necessary, public officials have historically in every industry stepped up to protect our constituents and consumers.

You have supported targeted regulations such as the Honest Ads Act, and that is an important step for election integrity. I am proud to be a cosponsor of that bill. But we need to address other broader issues as well. And today, you have said you would be open to some regulation, but this has been a pretty general conversation. So will you commit to working with Congress to develop ways of protecting constituent privacy and well-being, even if it means that that results in some laws that will require you to adjust your business model?

Mr. ZUCKERBERG. Senator, yes. We will commit to that. I think that that is an important conversation to have. Our position is not that regulation is bad. I think the Internet is so important in people's lives and it is getting more important.

Senator HASSAN. Yes.

Mr. ZUCKERBERG. The expectations on internet companies and technology companies overall are growing, and I think the real question is what is the right framework for this, not should there be one.

Senator HASSAN. That is very helpful, and I think the other question—and it does not just go to Facebook—is whether the framework should include financial penalties when large providers like Facebook are breached and privacy is compromised as a result because right now, there is very little incentive for whether it is Facebook or Equifax to actually be aggressive in protecting customer privacy and looking for potential breaches or vulnerabilities in their system. So what we hear after the fact, after people's privacy has been breached, after they have taken the harm that

comes with that and considerable inconvenience in addition to the harm. We have heard apologies but there is no financial incentive right now it seems to me for these companies to aggressively stand in their consumers' stead and protect their privacy, and I would really look forward to working with you on that and getting your considered opinion about it.

Mr. ZUCKERBERG. Well, Senator, we look forward to discussing that with you. I would disagree, however, that we have no financial incentive or incentive overall to do this. This episode has clearly hurt us and has clearly made it harder for us to achieve the social mission that we care about. And we now have to do a lot of work around building trust back, which is just a really important part of this.

[The information referred to follows:]

The other question I had, and it does not just apply to Facebook, is should the framework include financial penalties when large providers like Facebook are breached and privacy is compromised as a result? There is very little incentive for whether it is Facebook or Equifax to actually be abreast of protecting customer privacy and working for potential breaches or vulnerabilities in the system.

Protecting people's data is one of our most important responsibilities. We know that if people don't trust that their information will be safe on Facebook, they won't feel comfortable using our services.

We have every incentive to work as hard as we can to protect people's information, and we're committed to continuing our work to improve those protections.

Facebook is generally open to the idea of Federal breach notification requirements, particularly legislation that would centralize reporting and ensure a consistent approach across the United States. For example, in Europe, the GDPR requires notification to a lead supervisory authority, rather than individual member states, in cases of a data breach. In the United States, however, there is no centralized notification scheme, and instead, reporting obligations vary widely across all 50 states. This complexity makes it harder to respond appropriately and swiftly to protect people in the event of a data breach. We believe this is an important issue and an area that is ripe for thoughtful regulation.

Facebook is generally not opposed to regulation but wants to ensure it is the right regulation. We are already regulated in many ways—for example, under the Federal Trade Commission Act—and we are subject to ongoing oversight by the FTC under the terms of a 2011 consent order. Facebook has inherent incentives to protect its customers' privacy and address breaches and vulnerabilities. Indeed, the recent discovery of misconduct by an app developer on the Facebook platform clearly hurt Facebook and made it harder for us to achieve our social mission. As such, Facebook is committed to protecting our platform from bad actors, ensuring we are able to continue our mission of giving people a voice and bringing them closer together. We are also actively building new technologies to help prevent abuse on its platform, including advanced AI tools to monitor and remove fake accounts. We have also significantly increased our investment in security, employing more than 15,000 individuals working solely on security and content review and planning to increase that number to over 20,000 by the end of the year. We have also strengthened our advertising policies, seeking to prevent discrimination while improving transparency.

Senator HASSAN. Well, I thank you. My time is up, and I will follow up with you on that.

Chairman GRASSLEY [presiding]. Senator Capito.

STATEMENT OF HON. SHELLEY MOORE CAPITO, U.S. SENATOR FROM WEST VIRGINIA

Senator CAPITO. Thank you, Chairman Grassley.

And thank you, Mr. Zuckerberg, for being here today.

I want to ask just kind of a process question. You have said more than a few times that Facebook users can delete from their own account at any time. Well, we know in the course I do. I have got

grandchildren now, but children, you tell your children once you make that mark in the Internet system, it never really goes away.

So my question to you is, and I think you answered that once an individual deletes the information from their page, it is gone forever from Facebook's archives. Is that correct?

Mr. ZUCKERBERG. Yes. And I think you raise a good point, though, which is that we will delete it from our systems, but if you have shared something to someone else, then we cannot guarantee that they do not have it somewhere else.

Senator CAPITO. OK. So if somebody leaves Facebook and then rejoins and asks Facebook can you recreate my past, your answer would be?

Mr. ZUCKERBERG. If they delete their account, their answer is no. That is why we actually offer two options. We offer deactivation, which allows you to shut down or suspend your account but not delete the information because actually a lot of people want to at least for some period of time—and we hear students with exams coming up want to not be on Facebook because they want to make sure they can focus on the exam, so they deactivate their account temporarily but then want the ability to turn it back on when they are ready.

You can also delete your account, which is wiping everything, and if you——

Senator CAPITO. So?

Mr. ZUCKERBERG.—do that, then you cannot get it back.

Senator CAPITO. You cannot get it back? It is gone from your archives?

Mr. ZUCKERBERG. Yes.

Senator CAPITO. But is it ever really gone?

Mr. ZUCKERBERG. From our systems it is.

Senator CAPITO. From the cloud or wherever it is. I mean, it always seems to be able to reappear in investigations and other things, not necessary Facebook but other e-mails and other things of that nature.

What about the information going from the past, the information that has already been in the Cambridge Analytica case? You cannot really go back and redo that, so I am going to assume that what we have been talking with and the improvements that you are making now at Facebook are from this point forward. Is that a correct assumption?

Mr. ZUCKERBERG. Senator, I actually do think we can go back in some cases, and that is why one of the things that I announced is that we are going to be investigating every single app that had access to a large amount of information before we lock down the platform in 2014. And if we find any pattern of suspicious activity, then we are going to go, do a full audit of their systems. And if we find that anyone is improperly using data, then we will take action to make sure that they delete the data, and we will inform everyone who may have had their data misused.

Senator CAPITO. OK. The other suggestion I would make because we are kind of running out of time here is you have heard more than a few complaints, and I join the chorus, of the lapse in the time of when you discovered and when you became transparent. And I understand you sent out two messages just today to users.

So I would say—you say you regret that decision that you wish you had been more transparent at the time, so I would imagine if in the course of your investigation you find more breaches, so to speak, that you will be re-informing your Facebook customers?

Mr. ZUCKERBERG. Yes, that is correct. We have already committed that if we find any improper use, we will inform everyone affected.

Senator CAPITO. OK. Thank you. You have said also that you want to have an active view on controlling your ecosystem. Last week, the FDA Commissioner Scott Gottlieb addressed a drug summit in Atlanta and spoke on the national opioid epidemic. My state, and I am from West Virginia, and thank you for visiting. And next time you visit if you would please bring some fiber because we do not have connectivity in our rural areas like we really need, and Facebook could really help us with that.

So Commissioner Gottlieb called upon social media and internet service providers, and he mentioned Facebook when he talked about it, to try to disrupt the sale of illegal drugs and particularly powerful opioid fentanyl, which has been advertised and sold online. I know you have policies against this. The Commissioner is announcing his intention to convene a meeting of chief executives and senior leaders, and I want to know, could I get a commitment from you today that Facebook will commit to having a representative with Commissioner Gottlieb to finalize with this meeting?

Mr. ZUCKERBERG. Senator, that sounds like an important initiative, and we will send someone.

[The information referred to follows:]

Please send someone to the opioid meeting.

Thank you for highlighting this important issue. Yes, we will work with the Administration to send a Facebook representative. We are committed to doing our part in combating the opioid crisis and look forward to a continued dialogue with you.

Senator CAPITO. OK. And?

Mr. ZUCKERBERG. And let me also say that on your point about connectivity, we do have a group in Facebook that is working on trying to spread Internet connectivity in rural areas, and we would be happy to follow up with you on that as well. That is something that I am very passionate about.

Senator CAPITO. That is good. That is good news.

The last question I have just on the advertising, if somebody advertises on Facebook and somebody purchases something, does Facebook get a percentage or any kind of a fee associated with a successful purchase from an advertiser?

Mr. ZUCKERBERG. Senator, no. The way that the system works is advertisers bid how much it is worth it to them to show an ad or when an action happens. So it is not that we would get a percent of the sale, but—let us just use an example. So let us say you are an app developer, and your goal is you want to get more people to install your app. You could bid in the ad system and say I will pay $3 any time someone installs this app, and then we basically calculate on our side which ads are going to be relevant for people. And we have an incentive to show people ads that are going to be relevant because we only get paid when it delivers a business result. And that is how the system works.

Senator CAPITO. So you could be paid for the sale?

Mr. ZUCKERBERG. We get paid when the action that the advertiser wants to happen happens.

Senator CAPITO. All right. Thank you.

Chairman GRASSLEY. Senator Cortez Masto.

STATEMENT OF HON. CATHERINE CORTEZ MASTO, U.S. SENATOR FROM NEVADA

Senator CORTEZ MASTO. Thank you.

Mr. Zuckerberg, thank you. It has been a long afternoon, and I appreciate you being here and taking the time with every single one of us.

I am going to echo a lot of what I have heard my colleagues say today as well. I appreciate you being here, appreciate the apology, but stop apologizing and let us make the change. I think it is time to really change the conduct. I appreciate the fact that you talked about your principles for Facebook, notice to users on the use of the data and that users have complete control of their data. But the skepticism that I have—and I am hoping you can help me with this—is over the last, what, 7 years, 7, 14 years, 7 years, I have not seen really much change in ensuring that the privacy is there and that individual users have control over their data.

So let me ask you this. Back in 2009, you made two changes to your privacy policy, and in fact prior to that most users could either identify only friends or friends of friends as part of their privacy, correct, if they wanted to protect their data? They could identify only friends or friends of friends who could see their data, is that not correct?

Mr. ZUCKERBERG. Senator, I believe that we have had the option for people to share with friends, friends of friends, a custom audience, or publicly for a long time.

Senator CORTEZ MASTO. OK.

Mr. ZUCKERBERG. I do not remember exactly when we put that in place, but I believe it was before 2009.

Senator CORTEZ MASTO. So either you can choose only friends or friends of friends to decide how you are going to protect that data, correct?

Mr. ZUCKERBERG. Those are two of the options, yes.

Senator CORTEZ MASTO. OK. And in 2011 when the FTC started taking a look at this, they were concerned that if somebody chose only friends, that the individual user was under the impression they could continue to restrict sharing of data to limited audience, but that was not the case. And in fact, selecting friends only did not prevent users' information from being shared with their third-party applications their friends used. Is that not the case? And that is why the FTC was looking at you and making that change because there was concern that if you had friends on your page, a third party could access that information. Is that not correct?

Mr. ZUCKERBERG. Senator, I do not remember the exact context that the——

Senator CORTEZ MASTO. So let me help you here because David Vladeck, who spent nearly 4 years as Director of the Federal Trade Commission's Bureau of Consumer Protection, where he worked, including on the FTC's enforcement case against Facebook, basically identifies in this article that that was the case, that not only

did Facebook misrepresent and that is why there were eight counts of deceptive acts and practices, the actual FTC in November's 2011 Decree basically required Facebook to give users clear and conspicuous notice and to obtain affirmative—let me jump back here—to do three things. The decree barred Facebook from making any further deceptive privacy claims, and it required Facebook get consumers' approval before changing the way it shares their data. And most importantly, the third thing, it required Facebook to give users clear and conspicuous notice and to obtain affirmative express consent before sharing their data with third parties. That was part of the FTC consent decree, correct?

Mr. ZUCKERBERG. Senator, that sounds right to me.

Senator CORTEZ MASTO. OK. So at that time you were on notice that there were concerns about the sharing of data and information, users' data, including those friends with third parties, correct?

Mr. ZUCKERBERG. Senator, my understanding——

Senator CORTEZ MASTO. Well, let me ask you this. Let me do it this way. In response to the FTC consent to make those changes, did you make those changes? And what did you do to ensure individuals' user data was protected and they had notice of that information and that potentially third parties would be accessing that and they had to give express consent? What did you specifically do in response to that?

Mr. ZUCKERBERG. Senator, a number of things. One of the most important parts of the FTC consent decree that we signed was establishing a robust privacy program at the company headed by our chief privacy officer Erin Egan.

Senator CORTEZ MASTO. Can you give me——

Mr. ZUCKERBERG. We are now——

Senator CORTEZ MASTO.—specifics on it? And I have heard this over and over again and I am running out of time, but here is the concern that I have. It cannot be a privacy policy because that is what the consent said it could not be. It had to be something very specific, something very simple like you have heard from my colleagues, and that did not occur. Had that occurred, we would not be here today talking about Cambridge Analytica. Is that not really true? Had you addressed those issues then, had you done an audit, had you looked at not only the third party applications but they are audited their associated data storage as well, you would have known that this type of data information was being shared. And that is our concern, and that is what I am saying now. It is time just to make the change. It is time to really address the privacy issue. It is time to really come and lead the country on this issue and how we can protect individual user's data and information.

I know my time is running out, but I appreciate you being here, and I am just hoping that you are committed to working with us in the future in addressing these concerns.

Chairman THUNE [presiding]. Thank you, Senator Cortez Masto.

Senator Gardner.

STATEMENT OF HON. CORY GARDNER,
U.S. SENATOR FROM COLORADO

Senator GARDNER. Thank you, Mr. Chairman.

And thank you, Mr. Zuckerberg, for your patience and testimony today. The end is near I think, one, two, three, or four people, so that is good news to get out of this hearing.

A couple questions for you. To clarify one of the comments made about deleting accounts from Facebook, in the user agreement it says, "When you delete IP content, it is deleted in a manner similar to emptying the recycle bin on a computer. However, you understand that removed content may persist in backup copies for a reasonable period of time." How long is that?

Mr. ZUCKERBERG. Senator, I do not know sitting here what our current systems are on that, but the intent is to get all the content out of the system as quickly as possible.

Senator GARDNER. And does that mean your user data as well? It talks about IP content. Is that the same thing as your user data? It can sit in backup copies?

Mr. ZUCKERBERG. Senator, I think that that is probably right. I am not sitting here today having full knowledge of our current state of the systems around wiping all of the data out of backups, so I can follow up with you on that afterwards. But what I can tell you is that——

Senator GARDNER. But all backups get wiped?

Mr. ZUCKERBERG. That is certainly the way it is supposed to work.

Senator GARDNER. Has there ever been a failure of that?

Mr. ZUCKERBERG. Senator, I do not know. If we tell people that we are going to delete their data, we need to do that.

Senator GARDNER. And you do do that? Thank you.

Mr. Zuckerberg, a couple of other questions. I think that gets to the heart of this expectation gap as I call it with users. Facebook, as I understand it, if you are logged into Facebook with a separate browser and you log into another article, open a new tab in the browser while you have the Facebook tab open and that new tab has a Facebook, you know, button on it, you track the article that you are reading, is that correct?

Mr. ZUCKERBERG. Senator, I think that——

Senator GARDNER. In the tab?

Mr. ZUCKERBERG. I think that there is functionality like that, yes.

Senator GARDNER. Do you think users understand that?

Mr. ZUCKERBERG. Senator, I think that there is a reasonable—I think the answer is probably yes for the following reason: because when we show a like button on a website, we show social context there, so it says here are your friends who liked that. So in order to do that, we would have to——

Senator GARDNER. But if you have got your Facebook browser open and you open up an article in the *Denver Post* and it has a Facebook button it, do you think they know, consumers, users know that Facebook now knows what article you are reading in the *Denver Post*?

Mr. ZUCKERBERG. Well, we would need to have that in order to serve up the like button and show you who your friends were who had also liked that.

Senator GARDNER. So I think that goes to the heart of this expectation gap because I do not think consumers, users necessarily un-

derstand that. I mean, in going through this user agreement, as others have, you do need a lawyer to understand it. And I hope that you can close that expectation gap by simplifying the user agreement, making sure that people understand their privacy.

Has there ever been a violation outside of the talk about Cambridge Analytica about the privacy settings? Has a privacy setting violation ever occurred outside of Cambridge Analytica?

Mr. ZUCKERBERG. I am not aware that we have had systems that have——

Senator GARDNER. So the privacy setting——

Mr. ZUCKERBERG.—shown content——

Senator GARDNER.—a user uses have always been respected? There has never been an instance where those privacy settings have been violated?

Mr. ZUCKERBERG. That is my understanding. I mean, this is the core thing that our company does is you come to Facebook, you say, hey, I want to share this photo or I want to——

Senator GARDNER. I understand.

Mr. ZUCKERBERG.—send this message to these people and we have to——

Senator GARDNER. Has there ever been a breach of Facebook data, a hack?

Mr. ZUCKERBERG. There have been—I do not believe that there has been a breach of data that we are aware of.

Senator GARDNER. Has there ever been a hack?

Mr. ZUCKERBERG. Yes.

Senator GARDNER. And have those hacks accessed user data?

Mr. ZUCKERBERG. I do not believe so. I think we had an instance back in 2013 where someone was able to install some malware on a few employees' computers and had access to some of the content on their computers, but I do not believe——

Senator GARDNER. Never affected a user page?

Mr. ZUCKERBERG.—they had access to data.

Senator GARDNER. It never affected the user page?

Mr. ZUCKERBERG. I do not believe so.

Senator GARDNER. OK. Has the government ever asked to remove a page, have a page removed?

Mr. ZUCKERBERG. Senator, I believe so.

Senator GARDNER. OK. Can you get a warrant to join a page to be on a page pretending you are a separate user, to be liked by that, to track what that person is doing? Do you need a warrant for that or can the government just do that, the FBI, anybody?

Mr. ZUCKERBERG. Senator, I am not sure I fully understand. You are saying to——

Senator GARDNER. We can follow up on that because I do have one final question I want to ask you. A couple days ago, I think Facebook talked about that it would label traditional advocacy as political ads. And, for instance, if the Sierra Club was to run a climate change ad, that would be labeled a political ad. If the Chamber of Commerce wanted to place an ad as the climate change regulations would have an impact and talk about that through an ad, that would be labeled as political, which is different than current standards of what is political, what is issue advocacy. Is it your in-

tent to label things political that would be in contradiction to Federal law?

Mr. ZUCKERBERG. Senator, the intent of what we are trying to get at is the foreign election interference that we have seen has taken more the form of issue ads than direct political electioneering advertising. So, because of that, we think it is very important to extend the verification and transparency to issue ads in order to block the kind of interference that the Russians attempted to do and I think will likely continue to attempt to do. That is why I think that those measures are important to do.

Senator GARDNER. Thank you.

Chairman THUNE. Thank you, Senator Gardner.

Senator Tester.

STATEMENT OF HON. JON TESTER,
U.S. SENATOR FROM MONTANA

Senator TESTER. Thank you, Mr. Chairman.

I want to thank you for being here today, Mark. I appreciate you coming in. I hope this is not the last time we see you in front of committee. I know we are approaching 5 hours, so it has been a little tenuous, some mental gymnastics for all of us, and I just want to thank you for being here.

Facebook is an American company, and with that I believe you have got a responsibility to protect American liberties central to our privacy. Facebook allowed a foreign company to steal private information. They allowed a foreign company to steal private information from tens of millions of Americans largely without any knowledge of their own. Who and how we choose to share our opinions is a question of personal freedom. Who we share our likes and dislikes with is a question of personal freedom. This is a troubling episode that completely shatters that liberty, so that you understand the magnitude of this. Montanans are deeply concerned with this breach of privacy and trust.

So you have been at this for nearly 5 hours today. So besides taking reactive steps—and I want you to be as concise as you possibly can—what are you doing to make sure what Cambridge Analytica did never happens again?

Mr. ZUCKERBERG. Thank you, Senator. There are three important steps that we are taking here. For Cambridge Analytica, first of all, we need to finish resolving this, by doing a full audit of their systems to make sure that they delete all the data that they have and so we can fully understand what happened.

There are two sets of steps that we are taking to make sure that this does not happen again. The most important is restricting the amount of access to information that developers will have going forward. The good news here is that back in 2014 we actually had already made a large change to restrict access on the platform that would have prevented this issue with Cambridge Analytica from happening again today. Clearly, we did not do that soon enough. If we had done it a couple of years earlier, then we probably would not be sitting here today. But this is not a change that we had to take now in 2018. It is largely a change that we did back in 2014.

Senator TESTER. OK.

Mr. ZUCKERBERG. There are other parts of the platform that we also similarly can lock down now to make sure that other issues that might have been exploited in the future will not be able to. And we have taken a number of those steps, and I have outlined those in my written statement as well.

Senator TESTER. I appreciate that. And you feel confident that the actions that you have taken thus far, whether it was the ones back in 2014 or the one that you just talked about, about locking down the other parts, will adequately protect the folks who use Facebook?

Mr. ZUCKERBERG. Senator, I believe so——

Senator TESTER. OK.

Mr. ZUCKERBERG.—although security is never a solved problem.

Senator TESTER. That is all I need. You talked about a full audit of Cambridge Analytica's systems. Can you do a full audit if that information is stored in some other country?

Mr. ZUCKERBERG. Senator, right now, we are waiting on the audit because the U.K. Government is doing a government investigation of them.

Senator TESTER. OK. But——

Mr. ZUCKERBERG. And I do believe that the government will have the ability to get into the systems even if we cannot.

Senator TESTER. If information is stored in the U.K., but what if it is stored in some other country? What if the information is stored in some other country? Is an audit even possible?

Mr. ZUCKERBERG. Well, Senator, we believe a bunch of the information that we will be able to audit. I think you raise an important question, and if we have issues, then we—if we are not able to do an audit to our satisfaction, we are going to take legal action to enable us to do that. And also, I know that the U.K. and U.S. Governments are also involved in working on this as well.

Senator TESTER. I am telling you I would have faith in the U.S. Government. I really actually have faith in the U.K., too. There have been claims that this information is being stored in Russia. I do not care. It could be stored anywhere in the world. I do not know how you get access to that information. I am not as smart as you are about tech information, and so the question really becomes—and I have got to move on, but the question is I do not see how you can perform a full audit if they have got stuff stored somewhere else that we cannot get access to. That is all. Maybe you have other ideas on how to do that.

Mr. ZUCKERBERG. Well, I think we will know once we get in there whether we feel like we can fully investigate everything.

Senator TESTER. Just real quickly, Senator Schatz asked a question earlier about data and who owns the data. I want to dig into it a little bit more. You said—and I think multiple times during this hearing—that I own the data on Facebook if it is my data.

Mr. ZUCKERBERG. Yes.

Senator TESTER. And I am going to tell you that I think that that sounds really good to me, but in practice, let us think about this for a second. You are making about 40 billion bucks a year on the data. I am not making any money on it. It feels like you own the data. And in fact, I would say that the data that was breached through Cambridge Analytica, which impacted—and correct me if

these numbers are wrong—some 80 million Americans, my guess is that few if any knew that that information was being breached. If I own that data, I know it is being breached.

So could you give me some sort of idea on how you can really honestly say it is my data when, quite frankly, they may have goods on me. I do not want them to have any information on me.

Mr. ZUCKERBERG. Senator, when I say it is——

Senator TESTER. If I own it, I can stop it.

Mr. ZUCKERBERG. Yes. So, Senator, when I say it is your data, what I mean is that you have control over how it is used on Facebook. You clearly need to give Facebook a license to use it within our system——

Senator TESTER. Yes.

Mr. ZUCKERBERG.—or else the service does not work.

Senator TESTER. Yes, I know, and this license has been brought up many times today. And I am going to be quiet in just one second, Mr. Chairman.

But the fact is is the license is very thick, maybe intentionally so, so people get tired of reading it and do not want to.

Look, Mark, I appreciate you being here. I look forward to having you at another hearing.

Chairman GRASSLEY [presiding]. Senator Young.

STATEMENT OF HON. TODD YOUNG,
U.S. SENATOR FROM INDIANA

Senator YOUNG. Mr. Zuckerberg, thanks so much for being here enduring the many questions today. I think it is important you are here because your social media platform happens to be the ubiquitous social media platform. And there is not a Senator that you heard from today that is not on Facebook, that does not communicate with our constituents through Facebook. In a sense, we have to be on it, and so I think it is especially important that you are here not just for Facebook but really for our country and beyond.

The threshold question that continues to emerge here today is, what are the reasonable expectations of privacy that users ought to have? And, I will tell you, my neighbors are unsatisfied by an answer to that question that involves, you know, take a look at the User Agreement. And I think there has been a fair amount of discussion here about whether or not people actually read that User Agreement. I would encourage you to, you know, survey that, get all the information you can with respect to that, and make sure that user agreement is easy to understand and streamlined and so forth.

Mr. Zuckerberg, earlier in today's hearing, you drew a distinction that I thought was interesting. It caught my attention. It was a distinction between consumer expectation of privacy depending upon whether they were on an ISP or the pipes of the Internet as you characterized it or on an edge platform like Facebook. I find this distinction somewhat unsatisfying because most folks who use the Internet just think of it as one place if you will. They think of it as the Internet as opposed to various places requiring different degrees of privacy.

Could you speak to this issue and indicate whether you would support a comprehensive privacy policy that applies in the same manner to all entities across the entire internet ecosystem?

Mr. ZUCKERBERG. Senator, sure. I think that people's expectations of how they use these different systems are different. Some apps are very lightweight, and you can fully encrypt the data going across them in a way that the app developer or the pipes in the ISP case probably should not be able to see any of the content. And I think you probably should have a full expectation that no one is going to be introspecting or looking at that content. Other services——

Senator YOUNG. Give me some quick examples if you would kindly, sir.

Mr. ZUCKERBERG. Sure. Well, when data is going over the Verizon network, I think it would be good for that to be as encrypted as possible and such that Verizon would not look at it, right? I think that that is what people expect, and I do not know that being able to look at the data is required to deliver their service. That is how WhatsApp works, too, so that is an app. It is a very lightweight app. It does not require us to know a lot of information about you, so we can offer that with full encryption, and therefore, we do not see the content.

For a service like Facebook or Instagram where you are sharing photos and then people want to access them from lots of different places, people kind of want to store that in a central place so that way they can go access it from lots of different devices. In order to do that, we need to have an understanding of what that content is, so I think the expectations of what Facebook will have knowledge of versus what an ISP will have knowledge of are just different.

Senator YOUNG. I think that needs to be clearly communicated to your users, and we will leave it at that, that those different levels of privacy that the user can expect to enjoy when they are on your platform.

I would like to sort of take a different tack to internet privacy policy with you, sir. Might we create stronger privacy rights for consumers either through creating a stronger general property right regime online, say a new law that states unequivocally something that you have said before, that users own their online data or through stronger affirmative opt-in requirements on platforms like yours. Now, if we were to do that, would you need to retool your model if we were to adopt one of those two approaches?

Mr. ZUCKERBERG. Senator, could you repeat what the approaches are again?

Senator YOUNG. Yes, so one is to create a stronger property right for the individual online through a law that states unequivocally——

Mr. ZUCKERBERG. OK.

Senator YOUNG.—users own their data. The other one is a stronger affirmative opt-in requirement to be a user on Facebook. Would you have to fundamentally change the Facebook architecture to accommodate those policies?

Mr. ZUCKERBERG. Senator, those policies and the principles that you articulated are generally how we view our service already, so

depending on the details of what the proposal actually ends up being, and the details do just matter a huge amount here, it is not clear that it would be a fundamental shift. But the details really matter, and if this is something you are considering or working on, we would love to follow up with you on this because this is very important to get right.

[The information referred to follows:]

Might we create stronger privacy rights for consumers through creating a stronger general property right regime online, say a law states that users own their online data or stronger opt in requirements on platforms like yours? If we're to do that, would you need to retool your model? If we're to adopt one of the two approaches?

Our Terms of Service confirm that people own the information they shared on Facebook. They entrust it to us to use it consistent with our Terms and Data Policy to provide meaningful and useful services to them. They have the ability to choose who can see it, delete it, or take it with them if they want to do so. We're also rolling out a new Privacy Shortcuts feature, which centralizes a broad range of choices that people have about how their information is used as a part of the Facebook service, and we're contacting people on our service to ask them to make choices about these issues as well.

Facebook already allows users to download a copy of their information from Facebook. This functionality, which we've offered for many years, includes numerous categories of data, including About Me, Account Status History, Apps, Chat, Follower, Following, Friends, Messages, Networks, Notes, and more. We recently launched improvements to our "Download Your Information" tool, including to give people choices about whether they want to download only certain types of information and about the format in which they want to receive the download, to make it easier for people to use their information once they've retrieved it.

Of course, the details of any new privacy legislation matter, and we would be pleased to discuss any specific proposals with you and your staff.

Senator YOUNG. I would love to work with you. I am out of time. Thank you.

Chairman GRASSLEY. Senator Thune has a closing comment and——

Chairman THUNE. Yes.

Chairman GRASSLEY.—and I have a process statement for everybody to listen to.

Chairman THUNE. Mr. Chairman, thank you. And thanks to all of our Members for their patience. It has been a long hearing, a particularly long hearing for you, Mr. Zuckerberg. Thank you for sitting through this. But I think this is important.

I do have a letter here from the Motion Picture Association of America that I want to get into the record. Without objection.

Chairman GRASSLEY. Without objection, so ordered.

[The information referred to follows:]

April 10, 2018

Dear Chairmen Grassley and Thune, and Ranking Members Feinstein and Nelson:

Although many are understandably focusing on the privacy implications of the Facebook-Cambridge Analytica incident, I encourage you to also consider this event in a broader context: how online platforms are increasingly at the center of scandals with serious social, economic, consumer protection, and safety concerns, and how those scandals are beginning to overshadow these online platforms' benefits and erode public trust.

The internet has unquestionably revolutionized communication, commerce, and creativity. Yet there is a growing chorus of concern around a wave of problems resulting from a lack of online accountability.

In every other sector of our economy, the public rightfully expects companies to behave responsibly and to undertake reasonable efforts to prevent foreseeable harms associated with their products and services. When businesses fail to meet those obligations, they are ordinarily held accountable. For two decades, the internet has lived under a different set of rules and expectations, stemming largely from immunities and safe harbors put in place when the internet was in its infancy and looked nothing like it does today.

The internet is no longer nascent—and people around the world are growing increasingly uncomfortable with what it is becoming. As highlighted by the recent congressional debate around human trafficking, it is worth examining how we got to the point where some believe the rules simply don't apply and that platform immunity, whatever the cost, is the price the public must pay for a vibrant internet.

There was a vision for the internet, and this is not it. The moment has come for a national dialogue about restoring accountability on the internet. Whether through regulation, recalibration of safe harbors, or the exercise of greater responsibility by online platforms, something must change. I thank you for your leadership and look forward to working with you and your colleagues in the months ahead.

Respectfully submitted,

Charles H. Rivkin
Chairman & CEO
Motion Picture Association of America

cc: Members of the Senate Committee on Commerce, Science and Transportation
Members of the Senate Committee on the Judiciary

Chairman THUNE. And then just a quick, sort of, wrap-up question if you will and maybe one quick comment, but you have answered several questions today about efforts to keep bad actors, whether that is a terrorist group to a malicious foreign agent, off of your platform. You have also heard concerns about bias at Facebook, particularly bias against conservatives. And just as a final question, can you assure us that when you are improving tools to stop bad actors that you will err on the side of protecting speech, especially political speech, from all different corners?

Mr. ZUCKERBERG. Senator, yes. That is our approach. If there is an imminent threat of harm, we are going to take a conservative position on that and make sure that we flag that and understand that more broadly. But overall, I want to make sure that we provide people with the most voice possible. I want the widest possible expression, and I do not want anyone at our company to make any decisions based on the political ideology of the content.

Chairman THUNE. And just one final observation, Chairman Grassley. Mr. Zuckerberg has answered a lot of questions today, but there are also a lot of promises to follow up with some of our members and sometimes on questions about Facebook practices that seem fairly straightforward. I think it is going to be hard for us to fashion solutions to solve some of this stuff until we have some of those answers. And you had indicated earlier that you are continuing to try and find out who among these other analytics companies may have had access to user data that they were able to use. And hopefully, as you get those answers, you will be able to forward those to us, and it will help shape our thinking in terms of where we go from here.

But overall, I think it was a very informative hearing, Mr. Chairman, and so I am ready to wrap it up.

Chairman GRASSLEY. Yes. I probably would not make this comment, but your response to him in regard to political speech, I will not identify the CEO I had a conversation with yesterday, but one of our platforms, and he admitted to being more left than right—or, I mean, being left I guess is what he admitted. And I am not asking you what you are, but just so you understand that probably as liberals have a lot of concerns about, you know, the leaning of Fox News or conservatives have questions about the leaning of MSNBC let us say, it seems to me that when we get—whether it is from the right or the left, so I am speaking to you for your platform, there is a great deal of cynicism in American society about government generally.

And then when there are suspicions, legitimate or not, that maybe you are playing it one way unfairly toward the other, it seems to me that everything you do to lean over backwards to make sure that you are fair in protecting political speech, right or left, that you ought to do it. And I am not telling you how to do it, and I am not saying you do not do it, but we have got to do something to reduce this cynicism.

At my town meetings in Iowa, I always get this question: How come you guys in D.C. cannot get along, you know, meaning Republicans and Democrats. Well, I try to explain to them that they kind of get an obtuse—what would say—review of what goes on here because controversy makes news, so if people are getting along, you

never hear about that, so they get a distorted view of it. And really, Congressmen get along more than the public thinks.

But these attitudes of the public, we have got to change, and people of your position and your influence, you can do a lot to change this. I know you have got plenty of time to run your corporation. Through your corporation or privately, anything you can do to reduce this cynicism because we have a perfect Constitution—maybe it is not perfect, but we have got a very good Constitution and the longest written Constitution in the history of mankind. But if people do not have faith in the institutions of government and then it is our responsibility to enhance that faith so they have less cynicism on us, you know, we do not have a very strong democracy just because we have got a good Constitution.

So I hope that everybody will do whatever they can to help enhance respect for government, including speaking to myself, I have got to bend over backward to do what I can so I do not add to that cynicism. So I am sorry you had to listen to me.

[Laughter.]

Chairman GRASSLEY. And so this concludes today's hearing. Thanks to all the witnesses for attending. The record will be open for 14 days for the Members to submit additional written questions and for the witness, Mr. Zuckerberg, to make any corrections to his testimony.

The hearing is adjourned.

[Whereupon, at 7:24 p.m., the Committees were adjourned.]

A P P E N D I X

COMMITTEE FOR JUSTICE
Washington, DC, April 10, 2018

Hon. CHUCK GRASSLEY,
Chairman,
Senate Committee on the Judiciary.

Hon. DIANNE FEINSTEIN,
Ranking Member,
Senate Committee on the Judiciary.

RE: Facebook, Social Media Privacy, and the Use and Abuse of Data

Dear Chairman Grassley and Ranking Member Feinstein,

We write to you regarding your April 10 hearing, "Facebook, Social Media Privacy, and the Use and Abuse of Data." We, the president and public policy director of the Committee for Justice (CFJ), are concerned that the hearing will lead to the introduction of new legislation regulating online data collection and use. We are convinced such legislation is not only unnecessary but, if enacted, would also hurt consumers, threaten the online ecosystem that has transformed our daily lives, and negatively impact our country's economic growth.

Founded in 2002, CFJ is a nonprofit, nonpartisan legal and policy organization that educates the public and policymakers about and promotes the rule of law and constitutionally limited government. Consistent with this mission, CFJ engages in the national debate about a variety of tech policy issues, including advocating for digital privacy protections in Congress, the Federal courts, and the news media.[1]

We have concluded that a legislative solution to the data privacy issues being discussed at the hearing would be detrimental to our Nation for the following reasons:

- *Government-imposed restrictions on data collection would undercut economic growth, the vibrancy of the online ecosystem, and consumer satisfaction.* In recent decades, consumers' personal and professional lives have been transformed for the better by a vast collection of data-driven online resources that are made available to consumers for no cost because they are subsidized by advertising. These resources have also been an engine of economic growth, even during difficult economic times. For example, more than 70 million small businesses now use Facebook to grow and create jobs.[2] In particular, data-driven marketing, at issue in this hearing, is estimated to have added more than $200 billion to the U.S. economy in 2014, a 35 percent increase over just two years earlier.[3] Government-imposed restrictions on such marketing would slow or reverse this economic growth, while hurting consumers by causing the demise of many of the data-driven online resources they rely on.
- *Legislation designed to reign in big companies like Facebook will inevitably harm small companies and tech startups the most.* When regulations restrict companies' ability to collect and use data, advertisers and other online companies experience decreased revenue. Large companies can typically survive these decreases in revenue, while small companies are often driven out of business.

---

[1] *See, e.g.,* amicus briefs filed in *Carpenter v. United States.* August 2017. *https://www.scribd.com/document/356288790/Amicus-Brief-Filed-in-Carpenter-v-United-States* and *United States v. Kolsuz.* March 2017. *https://www.scribd.com/document/355249553/United-States-v-Kolsuz-Amucis-Brief;* Letter to Congress in support of the CLOUD Act. March 2018. *https://www.committeeforjustice.org/single-post/support-clarifying-lawful-use-data.*

[2] *Facebook: Transparency and Use of Consumer Data: Hearing Before the H. Comm. on Energy & Commerce,* 115th Cong. (2018) (statement of Mark Zuckerberg).

[3] Deighton, John and Johnson, Peter. "The Value of Data 2015: Consequences for Insight, Innovation and Efficiency in the U.S. Economy." Data & Marketing Association. Dec. 2015. *http://thedma.org/advocacy/data-driven-marketing-institute/value-of-data.*

The vast majority of Internet companies fall in the latter category and include the very companies that might otherwise grow to compete with and even supplant Facebook and the other tech giants of today. The European Union's Privacy and Electronic Communications Directive (2002/58/EC) provides an unfortunate example of the harm privacy regulations can inflict on small businesses.[4] It is one reason why there are relatively few technology start-ups in Europe and most of them struggle to receive venture capital funding.[5]

- *The best way to provide consumers with data privacy solutions that meet their needs is competition in the Internet marketplace.* In contrast, increased government regulation of data privacy will stifle competition, in part because only larger companies can afford the increased compliance costs and reductions in revenue. This hearing will undoubted include questions about balancing the tradeoffs between privacy and the ability to share our lives, make our voices heard, and build online communities through social media. It makes little sense for Congress to impose a one-size-fits-all answer to these questions, given that individuals value the tradeoffs very differently. Addressing data privacy through competition, on the other hand, allows consumers to answer these questions for themselves according to their individual values.
- *Public opinion polls showing support for stronger data protections are misleading because they rarely confront consumers with the monetary of and other costs of their choices.*[6] A 2016 study found that, despite most participants' unease with an e-mail provider using automated content analysis to provide more targeted advertisements, 65 percent of them were unwilling to pay providers any amount for a privacy-protecting alternative.[7] However, in the real world, consumers will lose free e-mail and social media if government-imposed privacy regulations cut into providers' advertising revenue. Moreover, such studies remind us that most consumers do not value data privacy enough to pay anything for it. That should not be too surprising considering that today's thriving but largely unregulated social media ecosystem is not something that was thrust upon consumers or arose from factors beyond their control. Instead, it arose through the collective choices and values tradeoffs of billions of consumers.
- *New, punitive data privacy legislation is unnecessary because legal safeguards already exist.* In addition to industry self-regulation, consumers of social media and other Internet services are protected by the Federal Trade Commission's vigorous enforcement of its data privacy and security standards, using the prohibition against "unfair or deceptive" business practices in Section 5 of the Federal Trade Commission Act 15 U.S.C. § 45(a).[8] In addition, state attorneys general enforce similar laws at the state level.[9]
- *The Cambridge Analytica incident that sparked this hearing must be put in perspective.* It is important to remember that the personal data disclosed by Facebook to an academic app builder named Aleksandr Kogan was not the sort of highly private data—credit card numbers, health records, and the like—that is sometimes stolen by hackers to the great detriment of consumers.[10] The data disclosed by Facebook came from the profiles of its users and consisted mostly

---

[4] OJ L 201, 31.7.2002, p. 37–47, ELI: *http://data.europa.eu/eli/dir/2002/58/oj.*

[5] Scott, Mark. "For Tech Start-Ups in Europe, an Oceanic Divide in Funding." The New York Times. January 19, 2018. *https://www.nytimes.com/2015/02/14/technology/for-tech-start-ups-in-europe-an-oceanic-divide-in-funding.html.*

[6] McQuinn, Alan. "The Economics of 'Opt-Out' Versus 'Opt-In' Privacy Rules." Information Technology and Innovation Foundation. Oct. 6, 2017. *https://itif.org/publications/2017/10/06/economics-opt-out-versus-opt-in-privacy-rules.*

[7] Strahilevitz, Lior Jacob, and Matthew B. Kugler. "Is Privacy Policy Language Irrelevant to Consumers?" *The Journal of Legal Studies* 45, no. S2. Sept. 9, 2016. *https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2838449.*

[8] *See, e.g.,* Federal Trade Commission. *FTC Staff Report: Self-regulatory Principles for Online Behavioral Advertising.* 2009. *https://www.ftc.gov/reports/federal-trade-commission-staff-report-self-regulatory-principles-online-behavioral;* Federal Trade Commission. *Privacy Online: Fair Information Practices in the Electronic Marketplace.* 2000. *http://www.ftc.gov/reports/privacy2000/privacy2000.pdf.*

[9] Widman, Amy, and Prentiss Cox. "State Attorneys General Use of Concurrent Public Enforcement Authority in Federal Consumer Protection Laws." *SSRN Electronic Journal,* 2011. doi:10.2139/ssrn.1850744.

[10] Iraklis Symeonidis, Pagona Tsormpatzoudi, and Bart Preneel. *Collateral Damage of Online Social Network Applications.* 2016. *https://eprint.iacr.org/2015/456.pdf;* Ruffini, Patrick. "The Media's Double Standard on Privacy and Cambridge Analytica." Medium. March 20, 2018. *https://medium.com/@PatrickRuffini/the-medias-double-standard-on-privacy-and-cambridge-analytica-1e37ef0649da.*

of names, hometowns, and page likes—in other words, the type of data most people on Facebook are public about.[11] However, even that data is no longer available to app developers today. Kogan got the idea before Facebook tightened its data privacy policies in 2014.[12] Finally, the concern that has focused so much attention on the Kogan incident—claims that the data was used by Cambridge Analytica to put Donald Trump over the top in 2016—have little basis in fact. Cambridge used the Facebook data to run voter-targeted ads for political campaigns, but it appears that those ads were neither effective nor used in the Trump campaign.[13]

- *Because there is no crisis requiring urgent action and because no one yet fully understands the extent and nature of the privacy risks posed by Facebook's now discontinued policies, calls for government-imposed regulation are premature.* Replacing the light-touch regulation of data privacy currently provided by the FTC and state law with more heavy-handed Federal legislation should be a last resort, not the reflexive response to news headlines. Consider also that the Cambridge Analytica incident would not be dominating the news but for the report, apparently incorrect, that the data in question was used to elect Donald Trump president.[14] Nor would the news coverage be so negative. Contrast that with the widely documented use of Facebook data in Barack Obama's 2012 presidential campaign, which was portrayed in a vastly different light by the news media and did not set off calls for Congressional hearings or new privacy legislation.[15] The important point is that allowing unhappiness with the 2016 election results to drive a push for increased government regulation and control of the Internet is a very bad way to make policy.
- *A rush to enact date privacy legislation is particularly dangerous in light of the glacial pace with which Congress will respond to the need for modernizing the legislation as technology rapidly evolves.* Consider the example of the Electronic Communications Privacy Act of 1986 (ECPA), which governs law enforcement's access to stored electronic data, such as e-mails. As storage of such data moved to the cloud, the ECPA became hopelessly obsolete, leading to increasingly concerned calls for its modernization from industry, law enforcement, and the White House. Despite those calls, it took many years for Congress to act by passing the Clarifying Lawful Overseas Use of Data or CLOUD Act in March of this year. And even then, Congress acted primarily because a Supreme Court case, *U.S. v. Microsoft,* forced them to.[16] There is good reason to believe that any legislation that comes out of this hearing will similarly remain in effect, unchanged, long after today's technological and privacy landscape has morphed into something we cannot fathom in 2018. In contrast, the self-regulation continuously being improved by Facebook and similar companies not only allows adaptation to technological change with far greater speed but also allows those companies to tailor data privacy solutions to the specific features of their platforms, rather than trying to conform with a one-size-fits-all Federal mandate.

---

[11] Albright, Jonathan. "The Graph API: Key Points in the Facebook and Cambridge Analytica Debacle." Medium. March 20, 2018. *https://medium.com/tow-center/the-graph-api-key-points-in-the-facebook-and-cambridge-analytica-debacle-b69fe692d747.*

[12] Facebook, "The New Facebook Login and Graph API 2.0." Facebook for Developers. April 30, 2014. *https://developers.facebook.com/blog/post/2014/04/30/the-new-facebook-login.*

[13] Kavanagh, Chris. "Why (almost) Everything Reported about the Cambridge Analytica Facebook 'Hacking' Controversy Is Wrong." Medium. March 26, 2018. *https://medium.com/@CKava/why-almost-everything-reported-about-the-cambridge-analytica-facebook-hacking-controversy-is-db7f8af2d042?mc_cid=849ab4c39f&mc_eid=5a60ec2d43.*

[14] *See, e.g.,* Wood, Paul. "The British Data-crunchers Who Say They Helped Donald Trump to Win." The Spectator. December 01, 2016. *http://www.spectator.co.uk/2016/12/the-british-data-crunchers-who-say-they-helped-donald-trump-to-win/;* Taggart, Kendall. "The Truth About The Trump Data Team That People Are Freaking Out About." BuzzFeed. February 16, 2017. *https://www.buzzfeed.com/kendalltaggart/the-truth-about-the-trump-data-team-that-people-are-freaking?utm_term=.it3kDeoJYn#.myDn1Kd9rJ;* Kroll, Andy. "Cloak and Data: The Real Story behind Cambridge Analytica's Rise and Fall." Mother Jones. March 26, 2018. *https://www.motherjones.com/politics/2018/03/cloak-and-data-cambridge-analytica-robert-mercer.*

[15] *See* Pilkington, Ed, and Amanda Michel. "Obama, Facebook and the Power of Friendship: The 2012 Data Election." The Guardian. February 17, 2012. *https://www.theguardian.com/world/2012/feb/17/obama-digital-data-machine-facebook-election;* Michael Scherer. "Friended: How the Obama Campaign Connected with Young Voters." TIME. November 20, 2012. *http://swampland.time.com/2012/11/20/friended-how-the-obama-campaign-connected-with-young-voters.*

[16] Levey, Curt. "Your e-mail privacy will get a boost thanks to the omnibus spending bill (and that's a good thing)." Fox News. March 22, 2018. *http://www.foxnews.com/opinion/2018/03/22/your-e-mail-privacy-will-get-boost-thanks-to-omnibus-spending-bill-and-thats-good-thing.html.*

In sum, rushing to enact new legislation regulating online data collection and use would hinder innovation in the rapidly evolving world of social media and data-driven marketing, lessen consumer choice, and negatively impact our Nation's economic growth.

We ask that this letter be entered in the hearing record. We thank you for your oversight of this important issue.

Sincerely,

CURT LEVEY,
President,
The Committee for Justice.

ASHLEY BAKER,
Director of Public Policy,
The Committee for Justice.

ITIF | INFORMATION TECHNOLOGY & INNOVATION FOUNDATION

ITIF on Zuckerberg Testimony: Facebook is Not the Problem, But It Can Be Part of the Solution

Daniel Castro | April 10, 2018

WASHINGTON—Ahead of Facebook CEO Mark Zuckerberg's testimony before the Senate Commerce, Science, and Transportation Committee and the Senate Committee on the Judiciary, the Information Technology and Innovation Foundation (ITIF), the world's top science and tech-policy think tank, released the following statement from ITIF Vice President Daniel Castro:

Facebook is not the problem, but it can be part of the solution. Facebook needs to demonstrate that it genuinely understands the real concerns its users have about how third-parties get access to their personal information, and it needs to take the necessary steps to ensure user data is protected.

But the U.S. should not blindly follow Europe's direction toward comprehensive data protection regulations. These strict rules have failed Europe, and they would kneecap the U.S. Internet economy, as well. Its light-touch approach to Internet regulation has made the U.S. digital economy the envy of the world. Taking steps toward European-style privacy regulation would offer only marginal value to users, but it would significantly erode U.S. competitiveness and Internet innovation.

Members of Congress should resist the urge to legislate how tech companies design their services. Instead, Members of Congress and regulators should hold Facebook accountable for its public commitments and past promises, and ensure that the company continues its transformation into a more responsible corporate citizen.

###

April 16, 2018

Dear Chairmen Grassley and Thune, and Ranking Members Feinstein and Nelson:

On behalf of the 17,000 members of the Directors Guild of America (DGA), 160,000 of SAG-AFTRA, and 140,000 of the International Alliance of Theatrical Stage Employees (IATSE), we thank you for advancing an important dialogue in our modern times. As you focus on the critical issue of privacy in the wake of the Facebook-Cambridge Analytica incident, we echo the concerns of the MPAA and others, and urge you to examine the situation in a broader context.

The internet is an incredibly important tool and provides substantial value to our members, the global economy and the general public. Yet there have been an increasing number of complex and troubling issues that have arisen lately related to the lack of accountability for online platforms. As new revelations mount, so too does our nation's cognitive dissonance between an internet that is an essential part of our daily lives, and one that signifies a breach of trust.

Originally meant to drive innovation, the early ground rules governing the internet were deliberately lax to encourage the experimentation deemed necessary for the growth of what was then a fledgling medium. However, with market valuations that now dwarf the GDPs of entire nations, today's Silicon Valley giants have the resources and capabilities to abide by the norms that apply to other corporations.

The ramifications have long been an unfortunate reality for our industry – film and television – which relies so heavily on strong copyright protections. The immunity of safe harbor for decades shielded internet companies from liability. Our members – armies of creators, performers, skilled craftspeople and workers who often dedicate weeks, months, even years of their lives to a single feature film or television series – have been among those hit hardest. We are also concerned about the massive privacy violations and threats that have been unleashed, particularly on performers and broadcasters, which are at record highs. Despite the fact that leading online players have matured into massive global companies, the rules still haven't changed.

We couldn't agree more that the time for a national conversation about accountability for online gatekeepers is now. We must delve into frank discussions about unintended consequences, and how they can be addressed. Our future depends on it. We thank you for your leadership and consideration, and welcome any questions you have.

Sincerely,

Russell Hollander
National Executive Director
Directors Guild of America

David P. White
National Executive Director
SAG-AFTRA

Matthew D. Loeb
International President
International Alliance of Theatrical Stage Employees

cc: Members of the Senate Committee on Commerce, Science and Transportation
Members of the Senate Committee on the Judiciary

CONTENT CREATORS COALITION

CreativeFuture
Creativity. Innovation. Tomorrow.

Independent Film & Television Alliance®

19 April 2018

The Honorable Chuck Grassley, Chairman
The Honorable Dianne Feinstein, Ranking Member
Senate Committee on the Judiciary
224 Dirksen Senate Office Building
Washington, DC 20510

The Honorable John Thune, Chairman
The Honorable Bill Nelson, Ranking Member
Senate Committee on Commerce, Science, and Transportation
512 Dirksen Senate Building
Washington DC, 20510

Dear Chairmen and Ranking Members:

On behalf of our combined membership of over 240,000 individuals and 670 companies, we want to thank you and your respective committees for leading last week's hearing where Facebook Chairman and CEO Mark Zuckerberg was questioned about the recent Cambridge Analytica data breach.

As representatives of the millions of Americans who work in the creative industries in every state in the union, we applaud your call for greater accountability by Facebook, as well as other Silicon Valley companies. As Chairman Thune recently observed, "tech companies have to understand that it's not the Wild West, and they have to exercise responsibility." Last week's hearing was an important first step in ensuring that Facebook, Google, Twitter, and other internet platforms must (1) take meaningful action to protect their users' data, (2) take appropriate responsibility for the integrity of the news and information on their platforms, and (3) prevent the distribution of unlawful and harmful content through their channels.

In last week's hearing, Mr. Zuckerberg stressed several times that Facebook must "take a broader view of our responsibility," acknowledging that it is "responsible for the content" that appears on its service and must "take a more active view in policing the ecosystem" it created. While most content on Facebook is not produced by Facebook, they are the publisher and distributor of immense amounts of content to billions around the world. As Senator Sullivan said in his line of questioning: "[T]here's some who are saying that [Facebook is] the world's biggest publisher. I think about 140 million Americans get their news

from Facebook." It is worth noting that a lot of that content is posted without the consent of the people who created it, including those in the creative industries we represent.

Mr. Zuckerberg characterizes Facebook's failure to take an appropriately broad view of its responsibility as a "big mistake" and promises that this will change. But if we are being honest, we must acknowledge that whether the lack of responsibility was a "mistake" or not, the failure of Facebook and others to take responsibility is rooted in decades-old policies, including legal immunities and safe harbors, that actually *absolve* internet platforms of accountability. We agree that change needs to happen – but we must ask ourselves whether we can expect to see real change as long as these companies are allowed to continue to operate in a policy framework that prioritizes the growth of the internet over accountability and protects those that fail to act responsibly. We believe this question must be at the center of any action Congress takes in response to the recent failures.

Accountability does not stop with Facebook, of course. Google, another major global platform that has long resisted meaningful accountability, also needs to step forward and endorse the broader view of responsibility expressed by Mr. Zuckerberg – as do many others. The real problem is not Facebook, or Mark Zuckerberg, regardless of how sincerely he seeks to own the "mistakes" that led to the hearing last week. The problem is endemic in a system that applies a different set of rules to the internet and fails to impose ordinary norms of accountability on businesses that are built around monetizing other people's personal information and content.

We can all appreciate the story of Facebook's founding in Mr. Zuckerberg's dorm room as a great moment in American entrepreneurialism. It's a lovely tale, but it's also history. Today's reality is that Facebook has monopoly power. It commands and determines the flow of both information and revenue for billions of people and businesses. It is understandable that Congress took a very light hand for decades to help nascent internet-based industries grow and prosper. But now Facebook and Google are grown-ups – and it is time they behaved that way.

Apologies are just words unless accompanied by action – from Facebook and other internet platforms. If they will not act, then it is up to you and your colleagues in the Senate to take action and not let these platforms' abuses continue to pile up.

We would be grateful if you would include this letter in the record for last week's hearing.

Sincerely,

American Federation of Musicians
Content Creators Coalition
CreativeFuture
Independent Film & Television Alliance

AVAAZ
THE WORLD IN ACTION

27 Union Square West, Suite 500
New York, NY 10003

How to Fix Fakebook Fast

After battling disinformation campaigns worldwide, Avaaz has consulted in depth with regulators, experts and social media executives on reform options while also polling its 46 million members.

Here are the 4 solutions which we we believe are legitimate, doable, and can be executed on a short timeline, as crucial elections worldwide approach in the fall.

1 **BAN THE BOTS – delete "Fakebook" by banning ALL fake or imposter user accounts.**

These accounts massively amplify disinformation campaigns, and they violate Facebook's own user policy. Facebook has disclosed that 270 million of its users are fake or duplicate accounts. They banned tens of thousands of fake accounts to protect French and German democracies before elections. They need to turn these one-off actions into ongoing and global policy.

2 **ALERT THE PUBLIC – notify all users EACH time they are exposed to fake or malicious content, and correct the record.**

To mitigate the public deception of disinformation campaigns, Facebook and other social networks need to alert individual users every time they view such content (not just share it, but view it), in posts that have at least equal prominence to the malicious content seen. False content needs to be clearly corrected with corrections endorsed by media that the user is most likely to trust.

3 **FUND THE FACT-CHECKERS – stand up an independent army big enough and fast enough to stem the spread of lies.**

While artificial intelligence is crucial, any system of correction must rely on a new industry of skilled, independent and trustworthy fact checkers. Funding models must protect the independence of this industry, which must rapidly expand beyond the current 6 nations to serve the public in all languages and countries.

4 **TELL THE TRUTH about fake users and disinformation campaigns, including through independent audits.**

We need to know just how bad things are, and be able to track progress. Facebook, Google, Twitter and social media must tell the whole truth about all the fake users, fake activity and disinformation campaigns on their platforms, through required full disclosures and independent audits the public can trust.

Avaaz.org/FixFakebook

RESPONSE TO WRITTEN QUESTIONS SUBMITTED BY HON. JOHN THUNE TO MARK ZUCKERBERG

Question 1. In its April 2, 2018, response to the letter Sen. Wicker, Sen. Moran, and I sent you on March 19, 2018, Facebook committed to investigating all apps that potentially had access to the same type of data as Cambridge Analytica to identify other misuses of such data. Will you commit to having Facebook brief Commerce Committee staff on a periodic basis regarding the progress of these investigations and any future developments in Facebook's efforts to combat data misuse more generally?

Answer. We are in the process of investigating every app that had access to a large amount of information before we changed our Platform in 2014. The investigation process is in full swing, and it has two phases. First, a comprehensive review to identify every app that had access to this amount of Facebook data and to focus on apps that present reason for deeper investigation. And second, where we have concerns, we will conduct interviews, make requests for information (RFI)—which ask a series of detailed questions about the app and the data it has access to—and perform audits using expert firms that may include on-site inspections. We have large teams of internal and external experts working hard to investigate these apps as quickly as possible. To date thousands of apps have been investigated and around 200 apps have been suspended—pending a thorough investigation into whether they did in fact misuse any data. Where we find evidence that these or other apps did misuse data, we will ban them and let people know.

These apps relate to a handful of developers: Kogan, AIQ, Cube You, the Cambridge Psychometrics Center, and myPersonality, with many of the suspended apps being affiliated with the same entity. Many of these suspensions include apps that appear to be "test" apps that were never released to the public, and therefore would not have acquired significant user data, although our investigation into these apps is ongoing.

Additionally, we have suspended an additional 14 apps, which were installed by around one thousand people. They were all created after 2014, after we made changes to more tightly restrict our platform APIs to prevent abuse. However, these apps appear to be linked to AIQ, which was affiliated with Cambridge Analytica. So, we have suspended them while we investigate further. Any app that refuses to take part in or fails our audit will be banned.

We will commit to briefing your staff on future developments.

Question 2. Mr. Zuckerberg, as you know, Sen. Wicker, Sen. Moran, and I sent a letter to you on March 19, requesting answers to several questions regarding Facebook's privacy practices. Facebook's general counsel sent a response letter on April 2nd that did not adequately answer some of the questions posed, saying that Facebook's review of the matter is ongoing. Will you commit to providing additional answers to our questions in writing in a timely manner as you learn more?

Answer. We responded to your questions to the best of our ability based on accessible data and information. Should additional or revised information related to the questions come to light, we respectfully request an opportunity to supplement or amend our response as needed.

Question 3. Mr. Zuckerberg, at the hearing you responded to over 20 questions from a number of Senators by saying that you would have to follow up at a later date. As you compile the promised information, please provide all such responses to these questions to Commerce Committee staff in addition to the Senator who posed the question.

Answer. Today we are submitting responses to the questions posed at the hearing requiring follow-up.

Question 4. Mr. Zuckerberg, given the concerns raised by a number of Senators that Facebook's user agreement is too opaque to give users a real understanding of how their data may be used and how they can control their data privacy, do you intend to make any changes to the user agreement? If so, please summarize those changes and why you believe they will make the agreement more easily understood.

Answer. We believe that it's important to communicate with people about the information that we collect and how people can control it. This is why we work hard to provide this information to people in a variety of ways: in our Data Policy, and in Privacy Basics, which provides walkthroughs of the most common privacy questions we receive. Beyond simply disclosing our practices, we also think it's important to give people access to their own information, which we do through our Download Your Information and Access Your Information tools, Activity Log, and Ad Preferences, all of which are accessible through our Privacy Shortcuts tool. We also provide information about these topics as people are using the Facebook service itself.

While "up front" information like that contained in the terms of service are useful, research overwhelmingly demonstrates that in-product controls and education are the most meaningful to people and the most likely to be read and understood. On-demand controls are also important, and we recently redesigned our entire settings menu on mobile devices from top to bottom to make things easier to find. We also created a new Privacy Shortcuts, a menu where users can control their data in just a few taps, with clearer explanations of how our controls work. The experience is now clearer, more visual, and easy-to-find.

Improving people's understanding of how digital services work is an industry-wide challenge that we are highly committed to addressing. That's why, over the last 18 months, we've run a global series of design workshops called "Design Jams," bringing together experts in design, privacy, law, and computer science to work collaboratively on new and innovative approaches. These workshops have run in Paris, London, Dublin, Berlin, Sao Paolo, Hong Kong, and other cities, and included global regulators and policymakers. At these workshops, expert teams use "people centric design" methods to create innovative new design prototypes and experiences to improve transparency and education in digital services. These workshops inform Facebook's constantly-improving approach.

In recognition of the need for improved approaches to data transparency across all digital services, working with partners from academia, design, and industry we recently launched TTC Labs, a design innovation lab that seeks to improve user experiences around personal data. TTC Labs is an open platform for sharing and innovation and contains insights from leading experts in academia, design and law, in addition to prototype designs from the Design Jams, template services and open-source toolkits for people-centric design for transparency, trust and control of data. Working collaboratively, and based on open-source approaches, TTC Labs seeks to pioneer new and more people-centric best practices for people to understand how their data is used by digital services, in ways that they find easy to understand and control.

Facebook is highly committed to improving people's experience of its own services as well as investing in new innovations and approaches to support improvements across the industry.

Question 5. Mr. Zuckerberg, in the weeks since the revelations regarding Cambridge Analytica, the Committee has become aware that Facebook has surveyed users about whether they trust the company to safeguard their privacy. Please provide the Commerce Committee with the results of any such survey.

Answer. Privacy is at the core of everything we do, and our approach to privacy starts with our commitment to transparency and control. Our threefold approach to transparency includes, first, whenever possible, providing information on the data we collect and use and how people can control it in context and in our products. Second, we provide information about how we collect and use data in our user agreements and related educational materials. And third, we enable people to learn more about the specific data we have about them through interactive tools such as Download Your Information, which lets people download a file containing data that they may want to take to another service, and Access Your Information, a tool we are launching that will let people more easily access and manage their data on Facebook.

Our approach to control is based on the belief that people should be able to choose who can see what they share and how their data shapes their experience on Facebook. People can control the audience for their posts and the apps that can receive their data. They can see and delete the history of their activities on Facebook, and, if they no longer want to use Facebook, they can delete their account and the data associated with it. Of course, we recognize that controls are only useful if people know how to find and use them. That is why we continuously deliver in-product educational videos in people's News Feeds on important privacy topics. We are also inviting people to take our Privacy Checkup—which prompts people to review key data controls—and we are sharing privacy tips in education campaigns off of Facebook, including through ads on other websites. To make our privacy controls easier to find, we are launching a new settings menu that features core privacy settings in a single place. We are always working to help people understand and control how their data shapes their experience on Facebook.

Question 6. Mr. Zuckerberg, when did you personally become aware of Cambridge Analytica's breach of your policies in 2014–2015, and when did you personally become aware that Cambridge Analytica had not in fact deleted the data they obtained despite certifying otherwise?

Answer. On December 11, 2015, *The Guardian* published an article reporting that Kogan and his company, GSR, may have passed information the app had obtained

from Facebook users to SCL Elections Ltd. (SCL)/Cambridge Analytica. As part of its investigation, Facebook contacted Kogan and Cambridge Analytica to investigate the allegations reflected in the reporting. Thereafter, Facebook obtained written certifications or confirmations from Kogan, GSR, and other third parties (including Cambridge Analytica and SCL) declaring that all such data they had obtained was accounted for and destroyed. In March 2018, Facebook received information from the media suggesting that the certification we received from SCL may not have been accurate and immediately banned SCL Group and Cambridge Analytica from purchasing advertising on our platform. Since then, Facebook has been actively investigating the issue, including pursuing a forensic audit of Cambridge Analytica, which is currently paused at the request of the UK Information Commissioner's Office (which is separately investigating Cambridge Analytica).

Mr. Zuckerberg did not become aware of allegations that Cambridge Analytica may not have deleted data about Facebook users obtained from Kogan's app until March of 2018, when these issues were raised in the media.

Question 7. On April 24, 2018, Facebook announced that it would institute an appeals process for posts that Facebook removes for violating its community standards. This process will initially only be available for posts that were removed for nudity/sexual activity, hate speech, or graphic violence. Why did Facebook decide to launch its appeals process for these categories? Prior to this new appeals process, did Facebook users have any recourse if their post was removed?

Answer. Prior to April 24, 2018, appeals generally were only available to people whose profiles, Pages, or Groups had been taken down, but we had not yet been able to implement an appeals process at the content level.

On April 24, we announced the launch of appeals for content that was removed for nudity/sexual activity, hate speech, and graphic violence. We focused on starting with these content violations initially based on feedback from our community.

We are working to extend this process further, by: supporting more violation types; giving people the opportunity to provide more context that could help us make the right decision; and making appeals available not just for content that was taken down, but also for content that was reported and left up.

Question 8. In your testimony, you discussed two typical business models employed by social media companies to make content available to users: an advertising-supported model and a subscription-based model. If Facebook were to shift from an advertising model to a subscription model, how much would consumers expect to pay in order to access Facebook content? Would you ever consider making such a shift? If not, why not?

Answer. Like many other free online services, we sell advertising space to third parties. Doing so enables us to offer our services to consumers for free. This is part of our mission to give people the power to build community and bring the world closer together.

Question 9. According to your testimony, Facebook has found that, while some users don't like advertisements, "people really don't like ads that aren't relevant" and the "overwhelming feedback we get from our community is that people would rather have us show relevant content." Can you elaborate on your basis for these statements about user preferences?

Answer. Part of Facebook's goal is to deliver the right content to the right people at the right time. This is just as true of posts and other content in users' News Feeds as it is for ads in their News Feed. And to choose the right ads Facebook listens to what feedback users provide. Users frequently provide feedback about what ads they want to see and don't want to see; they interact with ads positively (clicks, likes, comments, or shares) and negatively (by hiding the ad). Facebook takes all of this into consideration when selecting ads for its users.

In conjunction with this user feedback, Facebook has been working to better understand people's concerns with online ads. For example, Facebook has conducted multi-method, multi-market research surrounding ad blocking and personalization expectations among consumers. And the take away from this has been that people don't like to see ads that are irrelevant to them or that disrupt or break their experience. Furthermore, people like to have control over the kinds of ads they see. For these reasons, Facebook seeks to provide users more relevant ads, as well as the tools to improve their control over which ads they see.

Question 10. You stated that "there is some discomfort . . . with using information in making ads more relevant." Why do you believe Facebook users feel this discomfort? Do you believe users would feel more comfortable if they had a clearer understanding of the relationship between their information, the relevance of the advertisements they are served, and Facebook's ability to offer content without charging subscription fees?

Answer. We maintain our commitment to privacy by not telling advertisers who users are or selling people's information to anyone. That has always been true. We think relevant advertising and privacy are not in conflict, and we're committed to doing both well.

We believe targeted advertising creates value for people and advertisers who use Facebook. Being able to target ads to the people most likely to be interested in the products, service or causes being advertised enables businesses and other organizations to run effective campaigns at reasonable prices. This efficiency has particularly benefited small businesses, which make up the vast majority of the six million active advertisers on Facebook. That said, we are keenly aware of the concerns about the potential of our tools to be abused. That is why we are investing heavily in improving the security and integrity of our platform.

Separately, our core service involves personalizing all content, features and recommendations that people see on Facebook services. No two people have the same experience on Facebook or Instagram, and they come to our services because they expect everything they see to be relevant to them. If we were not able to personalize or select ads or other content based on relevance, this would fundamentally change the service we offer on Facebook—and it would no longer be Facebook.

We do not have a "business reason" to compromise the personal data of users; we have a business reason to protect that information. Our mission is to build community and bring the world closer together, but it is not enough to just connect people, we have to make sure those connections are positive. If people's experiences are not positive—if we fail to maintain their trust—they will not use our services.

Question 11. Mr. Zuckerberg, how does Facebook determine whether and for how long to store user data or delete user data?

Answer. In general, when a user deletes their account, we delete things they have posted, such as their photos and status updates, and they won't be able to recover that information later. (Information that others have shared about them isn't part of their account and won't be deleted.)

There are some limited exceptions to these policies: For instance, information can be accessed and preserved for an extended period when it is the subject of a legal request or obligation, governmental investigation, or investigations of possible violations of our terms or policies, or otherwise to prevent harm. We also retain information from accounts disabled for terms violations for at least a year to prevent repeat abuse or other term violations.

Question 12. Mr. Zuckerberg, you have discussed how a Facebook user can learn what data Facebook has collected about him or her. How can a non-user learn what data, if any, Facebook has collected about him or her?

Answer. If a person doesn't have a Facebook account but believes Facebook may have information about them, they can contact us to request a copy of their information. A contact form is available at *https://www.facebook.com/help/contact/180237885820953*. However, Facebook does not create profiles about or track web or app browser behavior of non-users.

Question 13. Does Facebook continue to track users who have turned off personalized ads? If so, why? Provide a list of uses Facebook makes of the data of users who have disabled personalized ads.

Answer. When people visit apps or websites that feature our technologies—like the Facebook Like or Comment button—our servers automatically log (i) standard browser or app records of the fact that a particular device or user visited the website or app (this connection to Facebook's servers occurs automatically when a person visits a website or app that contains our technologies, such as a Like button, and is an inherent function of Internet design); and (ii) any additional information the publisher of the app or website chooses to share with Facebook about the person's activities on that site (such as the fact that a purchase was made on the site). This is a standard feature of the Internet, and most websites and apps share this same information with multiple different third-parties whenever people visit their website or app. For example, the Senate Commerce Committee's website shares information with Google and its affiliate DoubleClick and with the analytics company Webtrends. This means that, when a person visits the Committee's website, it sends browser information about the visit to each one of those third parties. More information about how this works is available at *https://newsroom.fb.com/news/2018/04/data-off-facebook/*.

Question 14. Is Facebook's use of a user's data on the Facebook platform for targeted advertising a condition of using Facebook?

Answer. Users can't opt out of seeing ads altogether because selling ads is what keeps Facebook free, but they do have different options to control how their data can and can't be used to show them ads. They're all found in ad preferences, which

allows users to turn off the use of all data collected from partners off Facebook to target ads.

Users can also decide which of their profile fields they want used for ad targeting in the Information section under "About you." Users can remove themselves from interests under "Your interests" and categories under "Your categories."

Question 15. Mr. Zuckerberg, on March 25, you took out several full-page ads in newspapers around the world in which you stated: "We're also investigating every single app that had access to large amounts of data before we fixed this," referring to your 2014 policy changes. You went on to say, "We expect there are others. And when we find them, we will ban them and tell everyone affected." How many other offending apps have you found so far? You mentioned, when you find offending apps, you will be notifying users. Please also provide a list of these apps to Congress.

Answer. See Response to Question 1.

Question 16. Mr. Zuckerberg, as you may know, Carol Davidsen, who in 2012 served as the Obama campaign's director of data integration and media analytics, reportedly asserted that Facebook allowed the campaign to access users' personal data "because they were on our side." Did Facebook give preferential treatment to the Obama campaign with respect to data access in 2012? With respect to data access, did Facebook discriminate between the presidential campaigns in 2016?

Answer. Both the Obama and Romney campaigns had access to the same tools, and no campaign received any special treatment from Facebook. Likewise, we offered identical support to both the Trump and Clinton campaigns, and had teams assigned to both. Everyone had access to the same tools, which are the same tools that every campaign is offered.

Question 17. Since 2011, Facebook has been operating under a consent order issued by the Federal Trade Commission following agency charges that Facebook had deceived consumers by failing to keep privacy promises to them. You have indicated that—without prejudging the FTC's decision to investigate the Cambridge Analytica incident—you do not believe the consent order is implicated in the current matter. Please explain why.

Answer. We furnished extensive information to the FTC regarding the ability for users to port their Facebook data (including friends data that had been shared with them) with apps on Facebook's platform, as part of the FTC's investigation culminating in the July 27, 2012 Consent Order. The Consent Order memorializes the agreement between Facebook and the FTC and did not require Facebook to turn off the ability for people to port friends data that had been shared with them on Facebook to apps they used. Facebook voluntarily changed this feature of the Platform in 2014, however.

Among other things, the consent order obligates Facebook not to misrepresent the extent to which it maintains the privacy or security of covered information (Section I), not to materially exceed the restrictions of a privacy setting that applies to nonpublic user information without affirmative express consent (Section II), and to implement a comprehensive privacy program that is subjected to ongoing review by an independent assessor (Sections IV and V). Facebook accurately represented the operation of its developer Platform and the circumstances under which people could share data (including friends data) with developers, honored the restrictions of all privacy settings that covered developer access to data, and implemented a comprehensive privacy program build on industry-leading controls and principles, which has undergone ongoing review by an independent assessor approved by the FTC.

Question 18. Initial media reports stated that 50 million Facebook users were impacted by the Cambridge Analytica incident, Facebook later reported that 87 million users were impacted. How did Facebook arrive at this number, and can we expect this number to rise?

Answer. Facebook users shared some data associated with approximately 87 million users with Kogan's app, consisting of people who installed the app and the friends of those users whose settings permitted their data to be shared by their friends with apps. Facebook does not know how many of these users actually had data shared by Kogan with Cambridge Analytica, so this is a highly conservative estimate of the maximum number of users who could have been impacted. Several additional caveats apply to this figure:

- First, this figure does not include users who installed the app but have since deleted their Facebook account (since Facebook no longer has that information).
- Second, Facebook's counts of potentially affected friends of installers of the app are likely substantially higher than the "true" number of affected friends, because (a) the counts include any friend of any installer of the app during any time between when the app first became active on the Platform in November

2013 and when the app's access to friends data was limited in May 2015, even though the friend may not have been a friend when the app was actually installed by a relevant user; (b) the counts include any friend of any installer even if they changed their privacy settings during the relevant period to disallow sharing with apps installed by their friends (due to limited historical information about when or how users updated their settings), such that some of their data may not have been shared with the app; and (c) Facebook's counts include anyone who installed the app during its existence on Facebook's Platform, even if they installed the app at a time when its access to user data, including data from friends of installers, was more limited (due to limited historical information about when individual users installed the app).

In addition, it is worth noting that the existing evidence that we are able to access supports the conclusion that Kogan only provided SCL with data on Facebook users from the United States. While the accounts of Kogan and SCL conflict in some minor respects not relevant to this question, both have consistently maintained that Kogan never provided SCL with any data for Facebook users outside the United States. These consistent statements are supported by a publicly released contract between Kogan's company and SCL.

Question 19. Having discovered the improper data transfer to Cambridge Analytica in 2015, why did Facebook wait until 2018 to investigate or audit the data transfer to determine its full scope, including the type of data improperly transferred?

Answer. Facebook obtained written certifications from Kogan, GSR, and other third parties (including Cambridge Analytica and SCL) declaring that all data they had obtained, and any derivatives, was accounted for and destroyed. Based on recent allegations, we have reopened our investigation into the veracity of these certifications and have hired a forensic auditor to conduct a forensic audit of Cambridge Analytica's systems. We are currently paused on the audit at the request of the UK Information Commissioner's Office request, which is conducting a regulatory investigation into Cambridge Analytica (based in the UK), and we hope to move forward with that audit soon.

Facebook banned Cambridge Analytica from our service. We understand that the company is now defunct.

Question 20. Mr. Zuckerberg, as you know, the Commerce Committee has been seeking to find a bipartisan path forward on net neutrality legislation. I believe bipartisan legislation is the best way to protect net neutrality and stop the partisan back-and-forth at the Federal Communications Commission over this issue. Will you commit to working with Congress to develop a bipartisan legislative solution to the issue of net neutrality?

Answer. Keeping the Internet open for everyone is crucial. Not only does it promote innovation, but it lets people access information that can change their lives and gives voice to those who might not otherwise be heard. For these reasons, Facebook supports net neutrality and is open to working with members of Congress and anyone else on a solution that will preserve strong net neutrality protections.

RESPONSE TO WRITTEN QUESTIONS SUBMITTED BY HON. ROGER WICKER TO MARK ZUCKERBERG

Question 1. Mr. Zuckerberg, during the hearing you confirmed that Facebook collects the call and text histories of its users that use Android phones. You also stated that Facebook only collects call and text histories if a consumer opts-in to this Facebook service.

Does Facebook collect the call and text history information of minors (13 to 17 years of age) that have Android phones and opt-in to this service?

If yes, does Facebook require parental consent for minors to be able to opt-in to this service?

How and in what manner does Facebook disclose to its users that it is collecting the call and text history information of those that opt-in to this service?

Answer. Call and text history logging is part of an opt-in feature that lets people import contact information to help them connect with people they know on Facebook and Messenger. We introduced the call and text history component of this feature for Android users several years ago, and currently offer it in Messenger and Facebook Lite, a lightweight version of Facebook, on Android.

Contact importers are fairly common among social apps and serve as a way to more easily find the people users want to connect with. They help users find and

stay connected with the people they care about and provide them with a better experience across Facebook.

Before we receive call and text history from people, they specifically grant us permission to access this data on their device and separately agree to use the feature. If, at any time, they no longer wish to use this feature they can turn it off, and all previously shared call and text history shared via that app is deleted. People can also access information they previously imported through the Download Your Information tool.

We've reviewed this feature to confirm that Facebook does not collect the content of messages—and will delete all logs older than one year. In the future, people will only upload to our servers the information needed to offer this feature—not broader data such as the time of calls. We do allow people from 13 to 17 to opt into this service. However, we do take other steps to protect teens on Facebook and Messenger:

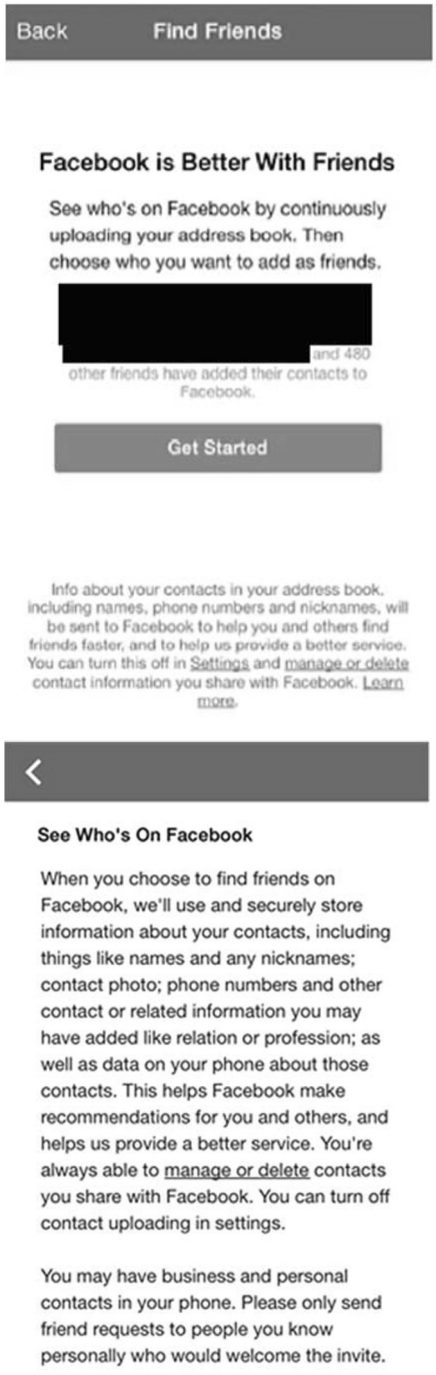
- We provide education before allowing teens to post publicly.
- We don't show search results based on specific profile data (high school, birthday/age, and hometown, or current city) of teens to unconnected adults when the adults search on Facebook.
- Unconnected adults can't message minors who are 13–17.
- We have age limits for advertisements. For example, ads for dating sites, financial services and other products or services are gated to users under 18. We've also helped many teenagers with information about bullying prevention campaigns and online safety tips, including creating a new website full of privacy and safety resources for teens: *https://www.facebook.com/safety/youth*

Question 2. Is the data Facebook collects from call and text histories of its users that have Android phones used for targeted advertising purposes?

Answer. No, Facebook does not use SMS history to target interest-based ads. Instead, call and text history logging is part of an opt-in feature for people using Messenger or Facebook Lite on Android. This helps Facebook users find and stay connected with the people they care about and provides them with a better experience across Facebook. This feature does not collect the content of users' calls or text messages.

Question 3. When a user uploads his or her contact list, Facebook collects the phone numbers of the user's contacts. Please provide all details regarding what Facebook does with the phone numbers of the users' contacts, including with whom Facebook shares those numbers, whether Facebook creates or updates profiles that associate these numbers with people's names, and how long Facebook stores those numbers.

Answer. Facebook allows people to upload, sync, and import their contacts, typically using permissions that are enabled by major operating systems like Apple's iOS and Google Android. When people use the contact upload tool, they see prompts explaining what data will be collected:


Back
Find Friends
Facebook is Better With Friends
See who's on Facebook by continuously uploading your address book. Then choose who you want to add as friends.
[redacted] and 480 other friends have added their contacts to Facebook.
Get Started
Info about your contacts in your address book, including names, phone numbers and nicknames, will be sent to Facebook to help you and others find friends faster, and to help us provide a better service. You can turn this off in Settings and manage or delete contact information you share with Facebook. Learn more.
See Who's On Facebook
When you choose to find friends on Facebook, we'll use and securely store information about your contacts, including things like names and any nicknames; contact photo; phone numbers and other contact or related information you may have added like relation or profession; as well as data on your phone about those contacts. This helps Facebook make recommendations for you and others, and helps us provide a better service. You're always able to manage or delete contacts you share with Facebook. You can turn off contact uploading in settings.
You may have business and personal contacts in your phone. Please only send friend requests to people you know personally who would welcome the invite.

We use this information that people choose to share for a variety of purposes, including to provide, personalize, and improve our products; provide measurement, analytics, and other business services; promote safety and security; to communicate with people who use our services; and to research and innovate to promote the social good. We provide more information in our Data Policy about these uses as well. People can view and manage their contact uploads using our Contacts Uploading tools, available at *https://www.facebook.com/help/355489824655936.*

Question 4. There have been reports that Facebook can track a user's internet-browsing activity even after the user has logged off of the Facebook platform. Can you confirm whether or not this is true?

If yes, how does Facebook disclose to its users that it is engaging in this type of tracking or data collection activity when a user has logged off of the Facebook platform?

Answer. When people visit apps or websites that feature our technologies—like the Facebook Like or Comment button—our servers automatically log (i) standard browser or app records of the fact that a particular device or user visited the website or app (this connection to Facebook's servers occurs automatically when a person visits a website or app that contains our technologies, such as a Like button, and is an inherent function of Internet design); and (ii) any additional information the publisher of the app or website chooses to share with Facebook about the person's activities on that site (such as the fact that a purchase was made on the site). This is a standard feature of the Internet, and most websites and apps share this same information with multiple different third-parties whenever people visit their website or app. For example, the Senate Commerce Committee's website shares information with Google and its affiliate DoubleClick and with the analytics company Webtrends. This means that, when a person visits the Committee's website, it sends browser information about their visit to each one of those third parties. More information about how this works is available at *https://newsroom.fb.com/news/2018/04/data-off-facebook/*.

When the person visiting a website featuring Facebook's tools is not a registered Facebook user, Facebook does not have information identifying that individual, and it does not create profiles for that individual.

We use the browser and app logs that apps and websites send to us—described above—in the following ways for non-Facebook users. First, these logs are critical to protecting the security of Facebook and to detecting or preventing fake account access. For example, if a browser has visited hundreds of sites in the last five minutes, that's a sign the device might be a bot, which would be an important signal of a potentially inauthentic account if that browser then attempted to register for an account. Second, we aggregate those logs to provide summaries and insights to websites and apps about how many people visit or use their product, or use specific features like our Like button—but without providing any information about a specific person. We do not create profiles for non-Facebook users, nor do we use browser and app logs for non-Facebook users to show targeted ads from our advertisers to them or otherwise seek to personalize the content they see. However, we may take the opportunity to show a general ad that is unrelated to the attributes of the person or an ad encouraging the non-user to sign up for Facebook.

When the individual is a Facebook user, we are also able to use this information to personalize their experiences on Facebook, whether or not they are logged out, but we will not target ads to users relying on this information unless the user allows this in their privacy settings. We do not sell or share this information with third-parties.

Question 5. Mr. Zuckerberg, if a user deletes his or her Facebook account, does Facebook still track that person on non-Facebook websites and applications?

Answer. Facebook does not create profiles or track website visits for people without a Facebook account. See Response to Question 4.

Question 6. Mr. Zuckerberg, you asserted in the hearing that "the expectations that people have" regarding use of data by ISPs are somewhat different than for edge platforms like yours. In fact, a survey by Peter D. Hart showed that 94 percent of consumers want their online data to be subject to a consistent level of privacy protection across the Internet and that ISPs and edge providers should be treated alike. Do you have any consumer survey data or empirical evidence to support your assertion that consumers expect or want different privacy protections for ISPs? If so, please provide the consumer survey data or empirical evidence that supports your assertion.

Answer. We believe that everyone should enjoy strong privacy protections, but we also realize that people have different expectations based on the context in which their information is provided. For instance, a person who orders shoes from a mail-

order catalog would expect the retailer to know what is in the box that he is being sent. But the customer would not expect the post office to know what he or she has purchased just because it is delivering the box. Because of this difference in expectations, the post office may need to do more to inform people if it intends to inspect packages it delivers and to give people control if it intends to use the information it learns in other ways.

Consistent with this difference, experts have observed, "The context in which broadband customers share private information with [Internet service] providers is specific and accompanied by cabined expectations: the customers share the information with [Internet service] providers to facilitate provision of a service for which they have contracted. The information is therefore most appropriately thought of as a loan to, rather than transferred to, broadband providers." [1] In contrast, a group of leading academic experts led by Prof. Nick Feamster of Princeton University observed that people may have access to only one or a few ISPs and simply expect those ISPs to deliver their communications. Such a person has no choice about whether to send his or her traffic over an ISP's network, whereas a "user may simply elect not to provide certain personal information or data to a social network, or even to not use the social network at all." [2] Other experts have observed that edge providers' collection of information is generally more expected because it is related to the services those companies provide.[3]

In our own services, Facebook needs to have a different understanding of a person's data than an ISP would. For instance, when someone adds information to their profile or likes a Page on Facebook, we must have access to that information in order to display it and use it to personalize that person's experience. People would not necessarily anticipate that other companies would have access to that information, which is why we do not sell people's information to advertisers and are increasing our efforts to guard against misuse of people's Facebook information by third parties. It is also why we provide people with the ability to turn off advertising based on the apps and websites they use outside of our service, and we are investing in enhanced transparency and control around this through our recent announcement of a new tool, Clear History, that we are building.

Although we have not reviewed the detailed survey by Mr. Hart to which the question refers, we understand that it focused on a different question than Mr. Zuckerberg's testimony. Specifically, Mr. Hart's survey asked people whether they believe that information should be subject to protection; this is different from asking whether people have different expectations about what information Facebook will receive when they put information on their Facebook profile, as compared to what information their Internet service provider will receive when they take the same action.

RESPONSE TO WRITTEN QUESTIONS SUBMITTED BY HON. ROY BLUNT TO MARK ZUCKERBERG

Question 1. Does Facebook collect user data through cross-device tracking, and does this include off-line data (offline data defined as that which is not directly contributed by a user through usage of features of the Facebook app)?

Answer. Yes, Facebook's Data Policy specifically discloses that we associate information across different devices that people use to provide a consistent experience wherever they use Facebook.

Facebook's services inherently operate on a cross-device basis: understanding when people use our services across multiple devices helps us provide the same personalized experience wherever people use Facebook—for example, to ensure that people's News Feeds or profiles contains the same content whether they access our services on their mobile phone or in a desktop computer's web browser.

In support of those and other purposes, we collect information from and about the computers, phones, connected TVs and other web-connected devices our users use that integrate with our Products, and we combine this information across a user's

---

[1] Comments of New America Foundation, FCC 16–39, at 7.

[2] Comments of Nick Feamster, *et al.,* FCC 16–39, at 3.

[3] Paul R. Gaus, *Only the Good Regulations Die Young: Recognizing the Consumer Benefits of the FCC's Now-Defunct Privacy Regulations,* 18 Minn. J. Law, Sci. & Tech. 713 (2017) ("Defining the Internet consumer seems like a facile task, but it must incorporate how the person uses digital devices to connect to the Internet and use content. In the context of ISPs, the digital consumer conforms to a traditional definition in that the consumer purchases ISP services to access the internet. In the space of edge providers, the digital consumer engages in traditional retail, watches content, interacts with others via social media, and performs a plethora of other activities that provide a telling summary about a person's life.").

different devices. For example, we use information collected about a person's use of our Products on their phone to better personalize the content (including ads) or features they see when they use our Products on another device, such as their laptop or tablet, or to measure whether they took an action in response to an ad we showed them on their phone or on a different device.

Information we obtain from these devices includes:

- Device attributes: information such as the operating system, hardware and software versions, battery level, signal strength, available storage space, browser type, app and file names and types, and plugins.
- Device operations: information about operations and behaviors performed on the device, such as whether a window is foregrounded or backgrounded, or mouse movements (which can help distinguish humans from bots).
- Identifiers: unique identifiers, device IDs, and other identifiers, such as from games, apps or accounts people use, and Family Device IDs (or other identifiers unique to Facebook Company Products associated with the same device or account).
- Device signals: Bluetooth signals, and information about nearby Wi-Fi access points, beacons, and cell towers.
- Data from device settings: information a user allows us to receive through device settings they turn on, such as access to their GPS location, camera, or photos.
- Network and connections: information such as the name of a user's mobile operator or ISP, language, time zone, mobile phone number, IP address, connection speed and, in some cases, information about other devices that are nearby or on their network, so we can do things like help them stream a video from their phone to their TV.
- Cookie data: data from cookies stored on a user's device, including cookie IDs and settings. More information is available at *https://www.facebook.com/policies/cookies/* and *https://help.instagram.com/1896641480634370?ref=ig.*

Advertisers, app developers, and publishers can send us information through Facebook Business Tools they use, including our social plug-ins (such as the Like button), Facebook Login, our APIs and SDKs, or the Facebook pixel. These partners provide information about a person's activities off Facebook—including information about their device, websites they visit, purchases they make, the ads they see, and how they use their services—whether or not they have a Facebook account or are logged into Facebook. For example, a game developer could use our API to tell us what games a person plays, or a business could tell us about a purchase a person made in its store. We also receive information about a person's online and offline actions and purchases from third-party data providers who have the rights to provide us with that person's information.

We use the information we have to deliver our Products, including to personalize features and content (including a person's News Feed, Instagram Feed, Instagram Stories, and ads) and make suggestions for a user (such as groups or events they may be interested in or topics they may want to follow) on and off our Products. To create personalized Products that are unique and relevant to them, we use their connections, preferences, interests and activities based on the data we collect and learn from them and others (including any data with special protections they choose to provide); how they use and interact with our Products; and the people, places, or things they're connected to and interested in on and off our Products.

For example, if people have shared their device locations with Facebook or checked into a specific restaurant, we can show them ads from an advertiser that wants to promote its services in their area or from the restaurant. We use location-related information-such as a person's current location, where they live, the places they like to go, and the businesses and people they're near-to provide, personalize and improve our Products, including ads, for them and others. Location-related information can be based on things like precise device location (if a user has allowed us to collect it), IP addresses, and information from their and others' use of Facebook Products (such as check-ins or events they attend). We store data until it is no longer necessary to provide our services and Facebook Products, or until a person's account is deleted—whichever comes first. This is a case-by-case determination that depends on things like the nature of the data, why it is collected and processed, and relevant legal or operational retention needs. We provide advertisers with reports about the kinds of people seeing their ads and how their ads are performing, but we don't share information that personally identifies someone (information such as a person's name or e-mail address that by itself can be used to contact

them or identifies who they are) unless they give us permission. For example, we provide general demographic and interest information to advertisers (for example, that an ad was seen by a woman between the ages of 25 and 34 who lives in Madrid and likes software engineering) to help them better understand their audience. We also confirm which Facebook ads led users to make a purchase or take an action with an advertiser.

Question 2. Cross-device data collection allows for data and user profile meshing that the average users are likely not cognizant of. Last year, the Federal Trade Commission flagged cross-device tracking as a possible concern, due to the fact that most companies do not explicitly discuss cross-device tracking in their privacy policies. Does Facebook disclose its collection methods across each applicable device, and if so, do you offer your users choices about how cross-device activity is tracked?

Answer. See Response to Question 1.

Question 3. Are users required to resubmit their permissions for each separate device that utilizes the Facebook app, or are user permissions blanketed across devices?

Answer. Mobile operating systems like Google's Android and Apple's iOS have device-specific access controls implemented at the operating system level.

Question 4. Facebook has been criticized for previous versions of its mobile application on Android devices, and the manner in which permissions were bundled without the ability to grant or deny each permission individually. I understand that Facebook and Android have updated their platforms, allowing more latitude for users to review permissions individually. What is the technical and commercial purpose of bundling permissions?

Answer. Android and other operating systems (like Apple's iOS) control the way device permissions work. Facebook can't, for example, request permissions in a way that's not permitted on an Android device. Accordingly, where permitted by the operating system, we generally ask for permission in-context—for example, requesting access to a device's camera roll when someone uses a feature that requires it. But for other permissions, on the Android operating system, we must list all of the permissions that various features might require at the point when a person installs the app, even if we do not intend to use those permissions until those features are accessed.

On our website, we explain more about permissions that we request and provide examples of how they are used. You can find this information at *https://www.facebook.com/help/210676372433246*.

Question 5. How does your company prioritize transparency and choice for users in the way that it collects and aggregates user data?

Answer. Our approach to transparency is threefold.

First, we provide information about the data we collect and use and how people can control it in context as people use Facebook. Research overwhelmingly demonstrates that in-product controls and education are the most meaningful to people and the most likely to be read and understood.

Second, we provide information about how we collect and use data in our user agreements and related educational materials. These materials include our Data Policy, which we updated recently to make it more detailed and easier to understand, and Privacy Basics, a series of short, interactive guides that answer some of the most common questions we receive about privacy.

Third, we enable people to learn more about the data we collect through interactive tools such as Download Your Information, which lets people download a file containing data that they may want to take to another service, and Access Your Information, a tool we've launched for people to more easily access and manage their data on Facebook.

Our approach to control is based on the belief that people should be able to choose who can see what they share and how their data shapes their experience on Facebook and should have control over all data collection and uses that are not necessary to provide and secure our service. People can control the audience for their posts and the apps that can receive their data. They can control the people, Pages, Groups, and Events they connect to, and how they see content from those connections in their News Feeds. They can provide feedback on every post they see on Facebook—feedback, for example, that they want to see less of a particular kind of post or fewer posts from a particular person or Page. They can see and delete the history of their activities on Facebook, and, if they no longer want to use Facebook, they can delete their account and the data associated with it.

We recognize, however, that controls are only useful if people know how to find and use them. That is why we continuously deliver in-product educational videos in people's News Feeds on important privacy topics like how to review and delete

old posts and what it means to delete an account. We are also inviting people to take our Privacy Checkup—which prompts people to review key data controls—and we are sharing privacy tips in education campaigns off of Facebook, including through ads on other websites. To make our privacy controls easier to find, we are launching a new settings menu that features core privacy settings in a single place.

RESPONSE TO WRITTEN QUESTIONS SUBMITTED BY HON. TED CRUZ TO MARK ZUCKERBERG

I. Directions

Please provide a wholly contained answer to each question. A question's answer should not cross-reference answers provided in other questions.

If a question asks for a yes or no answer, please provide a yes or no answer first and then provide subsequent explanation. If the answer to a yes or no question is sometimes yes and sometimes no, please state such first and then describe the circumstances giving rise to each answer.

If a question asks for a choice between two options, please begin by stating which option applies, or both, or neither, followed by any subsequent explanation.

If you disagree with the premise of a question, please answer the question as-written and then articulate both the premise about which you disagrees and the basis for that disagreement.

If you lack a basis for knowing the answer to a question, please first describe what efforts you undertook as Chief Executive Officer of Facebook order to ascertain an answer to the question and then provide your tentative answer as a consequence of its reasonable investigation. If even a tentative answer is impossible at this time, please state what efforts you and Facebook intend to take to provide an answer in the future and give an estimate as to when the Committees shall receive that answer.

If it is impossible to answer a question without divulging confidential or privileged information, please clearly state the basis for confidentiality or privilege invoked and provide as extensive an answer as possible without breaching that confidentiality or privilege. For questions calling for answers requiring confidential information, please provide a complete answer in a sealed, confidential form. These materials will be kept confidential. For questions calling for privileged information, please describe the privileged relationship and identify the privileged documents or materials that, if disclosed, would fully answer the question.

If the answer to a question depends on one or more individuals' memory or beliefs and that individual or those individuals either do not recall relevant information or are not available to provide it, please state the names of those individuals, what efforts you undertook to obtain the unavailable information, and the names of other individuals who may have access to that information.

To the extent that an answer depends on an ambiguity in the question asked, please state the ambiguity you perceive in the question and provide multiple answers which articulate each possible reasonable interpretation of the question in the light of the ambiguity.

To the extent that a question inquires about you or Facebook's actions, omissions, or policies, the question also asks about any entities that you or Facebook owns or controls, including any subsidiaries and affiliates. If context suggests that a question may ask about Facebook as a service rather than as an entity, please answer the question as applied to both Facebook as a service as well as all of Facebook's affiliated entities or platforms.

II. Questions

Question 1. Please attach a copy of each and every formal or informal policy, whether presently written or otherwise, regarding the moderation, promotion, evaluation, or alteration of users or content on Facebook. These include, for example, Facebook's Terms of Service, its Community Guidelines, and similar policies.

Answer. Facebook's Terms and Policies are available here: *https://www.facebook.com/policies*. Facebook's Community Standards are available at *https://www.facebook.com/communitystandards/*.

Question 2. Yes or no: Are Facebook's decisions to permit users access to its services or to permit content to remain displayed on its services, or the prominence or accessibility of that content, including its order, visibility, duration visible, inclusion in searches or order within search results, inclusion within "Trending" lists or analogous suggestions of content to users, determined in whole or part by Facebook's corporate values, beliefs, priorities, or opinions?

(a) Yes or no: Does Facebook promote, demote, or block users or content based on its assessment of the social value or social desirability of that content?

(b) Yes or no: Does Facebook promote, demote, or block users or content based on its assessment of that content's truth or falsity?

(c) Yes or no: Does Facebook promote, demote, or block users or content based on its assessment of the content's agreement or disagreement with Facebook's corporate values, beliefs, priorities, or opinions?

Answer. The conversations that happen on Facebook reflect the diversity and free expression of a community of more than two billion people communicating across countries and cultures and in dozens of languages, posting everything from text to photos and videos.

With regard the order and visibility of content, a user's News Feed is made up of stories from their friends, Pages they've chosen to follow and groups they've joined. *Ranking* is the process we use to organize all of those stories so that users can see the most relevant content at the top, every time they open Facebook. Ranking has four elements: the available *inventory* of stories; the *signals,* or data points that can inform ranking decisions; the *predictions* we make, including how likely we think they are to comment on a story, share with a friend, etc.; and a *relevancy score* for each story.

Misleading or harmful content on Facebook comes in many different forms, from annoyances like clickbait to hate speech and violent content. When we detect this kind of content in News Feed, there are three types of actions we take: remove it, reduce its spread, or inform people with additional context.

Our Community Standards and Ads Policies outline the content that is not allowed on the platform, such as hate speech, fake accounts, and praise, support, or representation of terrorism/terrorists. When we find things that violate these standards, we remove them. There are other types of problematic content that, although they don't violate our policies, are still misleading or harmful and that our community has told us they don't want to see on Facebook—things like clickbait or sensationalism. When we find examples of this kind of content, we reduce its spread in News Feed using ranking and, increasingly, we inform users with additional context so they can decide whether to read, trust, or share it.

The goal of our Community Standards is to encourage expression and create a safe environment. We base our policies on input from our community and from experts in fields such as technology and public safety. Our policies are also rooted in the following principles:

(1) Safety: People need to feel safe in order to build community. We are committed to removing content that encourages real-world harm, including (but not limited to) physical, financial, and emotional injury.

(2) Voice: Our mission is all about embracing diverse views. We err on the side of allowing content, even when some find it objectionable, unless removing that content can prevent a specific harm. Moreover, at times we will allow content that might otherwise violate our standards if we feel that it is newsworthy, significant, or important to the public interest. We do this only after weighing the public interest value of the content against the risk of real-world harm; and

(3) Equity: Our community is global and diverse. Our policies may seem broad, but that is because we apply them consistently and fairly to a community that transcends regions, cultures, and languages. As a result, our Community Standards can sometimes appear less nuanced than we would like, leading to an outcome that is at odds with their underlying purpose. For that reason, in some cases, and when we are provided with additional context, we make a decision based on the spirit, rather than the letter, of the policy.

Question 3. Yes or no: Have Facebook's decisions to permit users access to its services or to permit content to remain displayed on its services, or the prominence or accessibility of that content, including its order, visibility, duration visible, inclusion in searches or order within search results, inclusion within "Trending" lists or analogous suggestions of content to users, ever been determined in whole or part by Facebook's corporate values, beliefs, priorities, or opinions?

Answer. See Response to Question 2.

(a) Yes or no: Has Facebook ever promoted, demoted, or blocked users or content based on its assessment of the social value or social desirability of that content?

Answer. See Response to Question 2.

(b) Yes or no: Has Facebook ever promoted, demoted, or blocked users or content based on its assessment of that content's truth or falsity?

Answer. See Response to Question 2.

(c) Yes or no: Has Facebook ever promoted, demoted, or blocked users or content based on its assessment of the content's agreement or disagreement with Facebook's corporate values, beliefs, priorities, or opinions?

Answer. See Response to Question 2.

Question 4. Yes or no: Does Facebook employ its corporate values, beliefs, priorities, or opinions when deciding what content Facebook removes, republishes, moderates, promotes, or otherwise increases or decreases access to content?

Answer. The conversations that happen on Facebook reflect the diversity of a community of more than two billion people communicating across countries and cultures and in dozens of languages, posting everything from text to photos and videos.

We recognize how important it is for Facebook to be a place where people feel empowered to communicate, and we take our role in keeping abuse off our service seriously. That's why we have developed a set of Community Standards that outline what is and is not allowed on Facebook. Our Standards apply around the world to all types of content. They're designed to be comprehensive—for example, content that might not be considered hate speech may still be removed for violating our bullying policies.

The goal of our Community Standards is to encourage expression and create a safe environment. We base our policies on input from our community and from experts in fields such as technology and public safety. Our policies are also rooted in the following principles:

(1) Safety: People need to feel safe in order to build community. We are committed to removing content that encourages real-world harm, including (but not limited to) physical, financial, and emotional injury.

(2) Voice: Our mission is all about embracing diverse views. We err on the side of allowing content, even when some find it objectionable, unless removing that content can prevent a specific harm. Moreover, at times we will allow content that might otherwise violate our standards if we feel that it is newsworthy, significant, or important to the public interest. We do this only after weighing the public interest value of the content against the risk of real-world harm; and

(3) Equity: Our community is global and diverse. Our policies may seem broad, but that is because we apply them consistently and fairly to a community that transcends regions, cultures, and languages. As a result, our Community Standards can sometimes appear less nuanced than we would like, leading to an outcome that is at odds with their underlying purpose. For that reason, in some cases, and when we are provided with additional context, we make a decision based on the spirit, rather than the letter, of the policy.

Question 5. Yes or no: Has Facebook ever employed its corporate values, beliefs, priorities, or opinions when deciding what content Facebook removes, republishes, moderates, promotes, or otherwise increases or decreases access to content?

Answer. See Response to Question 4.

Question 6. It has become a common position on colleges and universities that statements which a listener disagrees with severely either can constitute violence or can rise to the moral equivalent of violence. According to this position, statements may rise to the level of violence even without a threat, reasonable or otherwise, of imminent violence, the use of "fighting words," or either a subjective intent or reasonably understood objective attempt to harass a listener.

(a) Yes or no: Does Facebook believe that speech neither advocating for physical violence against, threatening physical violence against, nor undertaken with either the subjective purpose or objective indicia of harassing a listener, may constitute violence?

Answer. Freedom of expression is one of our core values, and we believe that adding voices to the conversation creates a richer and more vibrant community. We want people to feel confident that our community welcomes all viewpoints and we are committed to designing our products to give all people a voice and foster the free flow of ideas and culture.

On the subject of credible violence, our Community Standards are explicit in what we don't allow. We aim to prevent potential real-world harm that may be related to content on Facebook. We understand that people commonly express disdain or disagreement by threatening or calling for violence in facetious and non-serious ways. That's why we try to consider the language, context and details in order to distinguish casual statements from content that constitutes a credible threat to public or personal safety. In determining whether a threat is credible, we may also consider additional information like a targeted person's public visibility and vulnerability. We remove content, disable accounts, and work with law enforcement when we believe there is a genuine risk of physical harm or direct threats to public safety.

(b) Yes or no: Has Facebook ever believed that speech neither advocating for physical violence against, threatening physical violence against, nor undertaken with either the subjective purpose or objective indicia of harassing a listener, may constitute violence?

Answer. See Response to Question 6(a).

Question 7. Regardless of Facebook's answer to Question 7, have any of Facebook's policies ever required removal of content not described in Question 7 from Facebook? If so, what categories, and based on what policies?

Answer. The goal of our Community Standards is to encourage expression and create a safe environment. We base our policies on input from our community and from experts in fields such as technology and public safety. Our policies are also rooted in the following principles:

(1) Safety: People need to feel safe in order to build community. We are committed to removing content that encourages real-world harm, including (but not limited to) physical, financial, and emotional injury.

(2) Voice: Our mission is all about embracing diverse views. We err on the side of allowing content, even when some find it objectionable, unless removing that content can prevent a specific harm. Moreover, at times we will allow content that might otherwise violate our standards if we feel that it is newsworthy, significant, or important to the public interest. We do this only after weighing the public interest value of the content against the risk of real-world harm; and

(3) Equity: Our community is global and diverse. Our policies may seem broad, but that is because we apply them consistently and fairly to a community that transcends regions, cultures, and languages. As a result, our Community Standards can sometimes appear less nuanced than we would like, leading to an outcome that is at odds with their underlying purpose. For that reason, in some cases, and when we are provided with additional context, we make a decision based on the spirit, rather than the letter, of the policy.

Question 8. Yes or no: Does Facebook consider itself a publisher or speaker entitled to First Amendment protection when supervising its services, designing or implementing its policies, altering, reposting, promoting or demoting content, including through results displayed by a user search, their order or presence in a "Trending" list or similar suggestions to users regarding content?

Answer. Facebook does not create the content that users share on its Platform, although it does take steps to arrange, rank and distribute that content to those who are most likely to be interested in it, or to remove objectionable content from its service. These activities are protected functions under Communications Decency Act Section 230 and the First Amendment.

Question 9. Aside from content clearly marked as coming from Facebook or one of its officers or employees, under what circumstances does Facebook consider itself as acting as a First-Amendment-protected publisher or speaker in its moderation, maintenance, or supervision over its users or their content?

Answer. We are, first and foremost, a technology company. Facebook does not create or edit the content that users publish on our platform. While we seek to be a platform for a broad range of ideas, we do moderate content according to published community standards in order to keep users on the platform safe, to reduce objectionable content and to make sure users participate on the platform responsibly.

Question 10. Yes or no: Does Facebook provide access to its services on a viewpoint-neutral basis? For this question and its subparts, please construe "access to its services" and similar phrases broadly, including the position or order in which content is displayed on its services, the position or order in which users or content show up in searches (or whether they show up at all), whether users or content are permitted to purchase advertisements (or be advertised), the rates charged for those advertisements, and so on.

Answer. We are committed to free expression and err on the side of allowing content. When we make a mistake, we work to make it right. And we are committed to constantly improving our efforts so we make as few mistakes as humanly possible.

Decisions about whether to remove content are based on whether the content violates our Community Standards.

Discussing controversial topics or espousing a debated point of view is not at odds with our Community Standards, the policies that outline what is and isn't allowed on Facebook. We believe that such discussion is important in helping bridge division and promote greater understanding.

We are committed to designing our products to give all people a voice and foster the free flow of ideas and culture. That said, when something crosses the line into

hate speech, it has no place on Facebook, and we are committed to removing it from our platform any time we become aware of it.

We define hate speech as a direct attack on people based on what we call protected characteristics—race, ethnicity, national origin, religious affiliation, sexual orientation, sex, gender, gender identity, and serious disability or disease. We also provide some protections for immigration status. We define attack as violent or dehumanizing speech, statements of inferiority, and calls for exclusion or segregation. The detailed guidelines our reviewers use to assess whether content violates our hate speech policies are available here: *https://www.facebook.com/communitystandards/objectionable_content/hate_speech*.

(a) Yes or no: Has Facebook ever discriminated among *users* on the basis of viewpoint when determining whether to permit a user to access its services? If so, please list each instance in which Facebook has done so.

Answer. See Response to Question 10.

(i) If so, does Facebook continue to do so today, or when did Facebook stop doing so?

Answer. See Response to Question 10.

(ii) If so, what viewpoint(s) has Facebook discriminated against or in favor of? In what way(s) has Facebook done so?

Answer. See Response to Question 10.

(iii) If so, does Facebook act only on viewpoints expressed on Facebook, or does it discriminate among users based on viewpoints expressed elsewhere? Has Facebook ever based its decision to permit or deny a user access to its services on viewpoints expressed off Facebook?

Answer. See Response to Question 10.

(b) Yes or no: Excluding content encouraging physical self-harm, threats of physical violence, terrorism, and other content relating to the credible and imminent physical harm of specific individuals, has Facebook ever discriminated among *content* on the basis of viewpoint in its services? If so, please list each instance in which Facebook has done so.

Answer. See Response to Question 10.

(c) Yes or no: Has Facebook ever discriminated against American users or content on the basis of an affiliation with a religion or political party? If so, please list each instance in which Facebook has done so and describe the group or affiliation against which (or in favor of which) Facebook was discriminating.

Answer. See Response to Question 10.

(d) Yes or no: Has Facebook ever discriminated against any American users or content on its services on the basis of partisan affiliation with the Republican or Democratic parties? This question includes advocacy for or against a party or specific candidate or official. If so, please list each instance and the party affiliation discriminated against.

Answer. See Response to Question 10.

(e) Yes or no: Has Facebook ever discriminated against any American users or content on its services on the basis of the user's or content's advocacy for a political position on any issue in local, State, or national politics? This question includes but is not limited to advocacy for or against abortion, gun control, consumption of marijuana, and net neutrality.

Answer. See Response to Question 10.

(f) Yes or no: Has Facebook ever discriminated against any American users or content on its services on the basis of the user's or content's religion, including advocacy for one or more tenets of that religion? If so, please list each such instance in which Facebook has done so and identify the religion, religious group, or tenet against which Facebook discriminated.

Answer. See Response to Question 10.

Question 11. Yes or no: Has Facebook ever discriminated between users in how their content is published, viewed, received, displayed in "trending" or similar lists, or otherwise in any function or feature, based on the user's political affinity, religion, religious tenets, ideological positions, or any ideological or philosophical position asserted? If so, please list each such incident as well as the basis on which Facebook discriminated against that user or content.

Answer. Being a platform for all ideas is a foundational principle of Facebook. We are committed to ensuring there is no bias in the work we do.

Suppressing content on the basis of political viewpoint or preventing people from seeing what matters most to them is directly contrary to Facebook's mission and our business objectives.

When allegations of political bias surfaced in relation to Facebook's Trending Topics feature, we immediately launched an investigation to determine if anyone violated the integrity of the feature or acted in ways that are inconsistent with Facebook's policies and mission. We spoke with current reviewers and their supervisors, as well as a cross-section of former reviewers; spoke with our contractor; reviewed our guidelines, training, and practices; examined the effectiveness of operational oversight designed to identify and correct mistakes and abuse; and analyzed data on the implementation of our guidelines by reviewers.

Ultimately, our investigation revealed no evidence of systematic political bias in the selection or prominence of stories included in the Trending Topics feature. In fact, our analysis indicated that the rates of approval of conservative and liberal topics are virtually identical in Trending Topics. Moreover, we were unable to substantiate any of the specific allegations of politically-motivated suppression of subjects or sources, as reported in the media. To the contrary, we confirmed that most of those subjects were in fact included as trending topics on multiple occasions, on dates and at intervals that would be expected given the volume of discussion around those topics on those dates.

Nonetheless, as part of our commitment to continually improve our products and to minimize risks where human judgment is involved, we are making a number of changes:

- We have engaged an outside advisor, former Senator Jon Kyl, to advise the company on potential bias against conservative voices. We believe this external feedback will help us improve over time and ensure we can most effectively serve our diverse community and build trust in Facebook as a platform for all ideas.
- We continue to expand our list of outside partner organizations to ensure we receive feedback on our content policies from a diverse set of viewpoints.
- We have made our detailed reviewer guidelines public to help people understand how and why we make decisions about the content that is and is not allowed on Facebook.
- We have launched an appeals process to enable people to contest content decisions with which they disagree.
- We are instituting additional controls and oversight around the review team, including robust escalation procedures and updated reviewer training materials.

These improvements and safeguards are designed to ensure that Facebook remains a platform for all ideas and enables the broadest spectrum of free expression possible.

Question 12. Except for accidental instances, has Facebook ever removed, downgraded, concealed, or otherwise censored content associated with any of the following? If yes, please describe the content that was removed, downgraded, concealed, or otherwise censored and the circumstances under which it was removed, downgraded, concealed, or otherwise censored.

a. Any individuals employed by Facebook?

b. Any elected official or candidate seeking elected office who self-identifies or is registered as a Democrat or a "Democratic Socialist"?

c. Any group who self-identifies as being part of the "Anti-Trump Resistance Movement"?

d. Any individuals employed by MSNBC?

e. Any individuals employed by CNN?

f. Any blogs that self-identify as "liberal" or "progressive"?

g. Any Facebook groups that self-identify as "liberal", "progressive", or being part of the "Anti-Trump Resistance Movement"?

h. Open Society Foundation?

i. Planned Parenthood?

j. Indivisible?

k. Sierra Club?

l. The American Civil Liberties Union?

m. The Anti-Defamation League?

n. The Council on American-Islamic Relations (CAIR)?

o. Emily's List?

p. NARAL Pro-Choice America?

q. The National Association for the Advancement of Colored People (NAACP)?

r. NextGen Climate Action?

s. The Southern Poverty Law Center?

t. The Union of Concerned Scientists?

u. Everytown for Gun Safety?

v. Amnesty International?

w. Priorities USA Action?

x. Media Matters for America?

y. Human Rights Watch?

z. Every Voice?

aa. NowThis?

bb. The Women's March?

cc. Organizing for America?

dd. Organizing for Action?

Answer. When content that violates our policies is brought to our attention, we remove that content—regardless of who posted it. We have removed content posted by individuals and entities across the political spectrum.

On April 24, 2018, we published the detailed guidelines our reviewers use to make decisions about reported content on Facebook. These guidelines cover everything from nudity to graphic violence.

We published these guidelines because we believe that increased transparency will provide more clarity on where we draw lines on complex and continuously evolving issues, and we hope that sharing these details will prompt an open and honest dialogue about our decision making process that will help us improve—both in how we develop and enforce our standards. We recognize that our policies are only as good as the strength and accuracy of our enforcement—and our enforcement is not perfect. We make mistakes because our processes involve people, and people are not infallible. We are always working to improve.

We do not typically comment on specific cases of content removal for privacy reasons.

Question 13. In your testimony before the committees, you stated several times that Facebook prohibits content based on its status as "hate speech." How have you and Facebook defined "hate speech" today and at any other stage in Facebook's existence?

Answer. We define hate speech as a direct attack on people based on what we call protected characteristics—race, ethnicity, national origin, religious affiliation, sexual orientation, sex, gender, gender identity, and serious disability or disease. We also provide some protections for immigration status. We define attack as violent or dehumanizing speech, statements of inferiority, and calls for exclusion or segregation. The detailed guidelines our reviewers use to assess whether content violates our hate speech policies are available here: *https://www.facebook.com/communitystandards/objectionable_content/hate_speech*.

Our Community Standards make an important distinction between targeting people and targeting particular beliefs or institutions. We believe that people should be able to share their views and discuss controversial ideas on Facebook.

Question 14. Did or does Facebook collaborate with or defer to any outside individuals or organizations in determining whether to classify a particular statement as "hate speech?" If so, please list the individuals and organizations.

Answer. Hate speech has no place on our platform. Our Community Standards prohibit attacks based on characteristics including race, ethnicity, religion, and national origin.

Facebook has partnerships with academics and experts who study organized hate groups and hate speech. These academics and experts share information with Facebook as to how organizations are adapting to social media and give feedback on how Facebook might better tackle these problems. We recently hosted several of these academics at Facebook for multiple days of observation and assessment, during which the academics attended substantive meetings on our content policies and the guidance we provide to our reviewers. Further, in the area of hate speech, there are very important academic projects that we follow closely. Timothy Garton Ash, for example, has created the Free Speech Debate to look at these issues on a cross-cultural basis. Susan Benesch established the Dangerous Speech Project, which investigates the connection between speech and violence. These projects show how much work is left to be done in defining the boundaries of speech online, which is why we will keep participating in this work to help inform our policies at Facebook.

We are committed to continuing our dialogue with third parties to ensure we can have the widest possible expression of ideas, while preventing abuse of the platform.

Facebook works with organizations from across the political spectrum around changes to our content standards including hate speech. While we do not share individual pieces of content from users with these organizations out of concerns for user privacy, we do provide in-depth examples and explanations of what the policy changes would entail.

Question 15. Did or does Facebook collaborate with or defer to any outside individuals or organizations in determining whether a given speaker has committed acts of "hate speech" in the past? If so, please list the individuals and organizations.

Answer. In an effort to prevent and disrupt real-world harm, we do not allow any organizations or individuals that are engaged in organized hate to have a presence on Facebook. We also remove content that expresses support or praise for groups, leaders, or individuals involved in these activities.

In developing and iterating on our policies, including our policy specific to hate speech, we consult with outside academics and experts from across the political spectrum and around the world. We do not, however, defer to these individuals or organizations in making decisions about content on our platform. Content that violates our Community Standards is removed when we are made aware of it, and content that doesn't violate is left on the platform.

Designating hate organizations and/or individuals is an extensive process that takes into account a number of different signals. We worked with academics and NGOs to establish this process and regularly engage with them to understand whether we should refine it. Among the signals we consider are whether the individual or organization in question has called for or directly carried out violence against people based on protected characteristics.

Question 16. Did or does Facebook ban or otherwise limit the content of individuals or organizations who have spoken "hate speech" on its platform aside from the offending content? If so, under what circumstances?

Answer. See Response to Question 15.

Question 17. Yes or no: Did or does Facebook ban or otherwise limit the content of individuals or organizations on its platform based on hate speech or other behavior conducted outside of Facebook's platform?

Answer. See Response to Question 15.

Question 18. Yes or no: Do you believe that "hate speech" is not protected under the First Amendment from government censorship?

Answer. The goal of our Community Standards is to encourage expression and create a safe community for our 2 billion users, more than 87 percent of whom are located outside the United States.

We err on the side of allowing content, even when some find it objectionable, unless removing that content prevents a specific harm.

We do not allow hate speech on Facebook because it creates an environment of intimidation and exclusion and in some cases may promote real-world violence.

Our current definition of hate speech is anything that directly attacks people based on what are known as their "protected characteristics"—race, ethnicity, national origin, religious affiliation, sexual orientation, sex, gender, gender identity, or serious disability or disease. However, our definition does allow for discussion around these characteristics as concepts in an effort to allow for and encourage expression and dialogue by our users.

There is no universally accepted answer for when something crosses the line.

Our approach to hate speech, like those of other platforms, has evolved over time and continues to change as we learn from our community, from experts in the field, and as technology provides us new tools to operate more quickly, more accurately and precisely at scale.

Question 19. Yes or no: Have you ever believed that "hate speech" is not protected under the First Amendment from government censorship?

Answer. See Response to Question 18.

Question 20. Yes or no: Does Facebook believe that "hate speech" is not protected under the First Amendment from government censorship?

Answer. See Response to Question 18.

Question 21. Yes or no: Has Facebook ever believed that "hate speech" is not protected under the First Amendment from government censorship?

Answer. See Response to Question 18.

Question 22. Yes or no: Does Facebook's "hate speech" policy prohibit, exclude, remove, or censor content that, were Facebook a governmental entity, would be entitled to First Amendment protections?

Answer. See Response to Question 18.

Question 23. Facebook states on its website that, per its community standards, Facebook will remove hate speech, which it describes as "including content that directly attacks people based on their: race, ethnicity, national origin, religious affiliation, sexual orientation, sex, gender, or gender identity, or serious disabilities or diseases." Yes or no: Does Facebook limit its definition of hate speech only to content that "directly attacks" people based on the aforementioned characteristics?

Answer. We define "attack" under our hate speech policy as violent or dehumanizing speech, statements of inferiority, and calls for exclusion or segregation. We allow discussion of issues related to characteristics like race, gender, ethnicity, and immigration status. We do not permit attacks against people based on these characteristics. Context matters in making what can be a difficult determination in some cases.

Specific details on the type of content that is prohibited under our hate speech policies are available here: *https://www.facebook.com/communitystandards/objectionable_content/hate_speech*.

Question 24. What standard or procedure has Facebook applied now and in the past in determining whether content "directly attacks" an individual or group based on a protected characteristic under Facebook's community standards?

Answer. See Response to Question 23.

Question 25. Yes or no: Has Facebook ever removed content for hate speech that did not directly attack a person on the basis of his or her race, ethnicity, national origin, religious affiliation, sexual orientation, sex, gender, or gender identity, or serious disabilities or diseases? If so, what criteria did Facebook use to determine that the content violated Facebook's policy?

Answer. We define "attack" under our hate speech policy as violent or dehumanizing speech, statements of inferiority, and calls for exclusion or segregation.

Sometimes, it's obvious that something is hate speech and should be removed—because it includes the direct incitement of violence against people possessing protected characteristics, or degrades or dehumanizes people. Sometimes, however, there isn't a clear consensus—because the words themselves are ambiguous, the intent behind them is unknown, or the context around them is unclear. Language also continues to evolve, and a word that was not a slur yesterday may become one today.

Here are some of the things we take into consideration when deciding what to leave on the site and what to remove.

- Context: Regional and linguistic context is often critical in deciding whether content constitutes hate speech, as is the need to take geopolitical events into account. In Myanmar, for example, the word "kalar" has benign historic roots, and is still used innocuously across many related Burmese words. The term can however also be used as an inflammatory slur, including as an attack by Buddhist nationalists against Muslims. We looked at the way the word's use was evolving, and decided our policy should be to remove it as hate speech when used to attack a person or group, but not in the other harmless use cases.
- Intent: There are times someone might share something that would otherwise be considered hate speech but for non-hateful reasons, such as making a self-deprecating joke or quoting lyrics from a song. People often use satire and comedy to make a point about hate speech. In other cases, people may speak out against hatred by condemning someone else's use of offensive language, which requires repeating the original offense. This is something we allow, even though it might seem questionable since it means some people may encounter material disturbing to them. But it also gives our community the chance to speak out against hateful ideas. We revised our Community Standards to encourage people to make it clear when they're sharing something to condemn it, but sometimes their intent isn't clear, and anti-hatred posts get removed in error.

On April 24, 2018, we announced the launch of appeals for content that was removed for hate speech. We recognize that we make enforcement errors on both sides of the equation—what to allow, and what to remove—and that our mistakes cause a great deal of concern for people, which is why we need to allow the option to request review of the decision and provide additional context that will help our team see the fuller picture as they review the post again. This type of feedback will allow us to continue improving our systems and processes so we can prevent similar mistakes in the future.

Question 26. Has Facebook ever removed content for hate speech that was posted by an individual employed by Facebook? If so, please describe each instance.

Answer. Our policies apply equally to all of our users. If a Facebook employee posted content that was reported to us and violated our policies, the content would be removed.

Question 27. Recording artist Taylor Swift recently released a cover of Earth, Wind & Fire's "September."

(a) In response, Nathaniel Friedman, an author at GQ magazine, stated that "Taylor Swift's cover of 'September' is hate speech." Does Facebook agree?

(b) In response, Monique Judge, an author at The Root, stated that "Taylor Swift needs her *** whooped." Is this statement hate speech?

Answer. We define hate speech as a direct attack on people based on what we call protected characteristics—race, ethnicity, national origin, religious affiliation, sexual orientation, sex, gender, gender identity, and serious disability or disease. We also provide some protections for immigration status. We define attack as violent or dehumanizing speech, statements of inferiority, and calls for exclusion or segregation. Our detailed hate speech policies are available at *https://www.facebook.com/communitystandards/objectionable_content/hate_speech*.

We generally do not assess whether content violates our policies (including our hate speech policy) unless it is part of our normal content review process. Context matters in making what can be a difficult determination in some cases. Sometimes, it's obvious that something is hate speech and should be removed—because it includes the direct incitement of violence against people possessing protected characteristics, or degrades or dehumanizes people. Sometimes, however, there isn't a clear consensus—because the words themselves are ambiguous, the intent behind them is unknown or the context around them is unclear. Language also continues to evolve, and a word that was not a slur yesterday may become one today.

Question 28. It was reported that Democratic D.C. Councilman Trayon White posted a video on his Facebook page blaming a recent snowstorm on wealthy Jewish families. According to *USA Today,* White said: "It just started snowing out of nowhere this morning, man. Y'all better pay attention to this climate control, man, this climate manipulation," which White attributed to "the Rothschilds controlling the climate to create natural disasters they can pay for to own the cities, man."

(a) Yes or no: Does Facebook consider this video or this quote hate speech?

Answer. See Response to Question 27.

(b) Yes or no: Did Facebook remove this video from its platform? If so, when? If not, why not?

Answer. See Response to Question 27.

Question 29. Multiple authors for the website Vox, including its founder, Ezra Klein, have described Charles Murray's book, *The Bell Curve,* as "hate speech." Similarly, the left-wing Southern Poverty Law Center perplexingly describes Murray as a "white nationalist," largely relying on its depiction of *The Bell Curve.*

(a) Does *The Bell Curve* qualify as "hate speech" for purposes of Facebook's policies?

Answer. See Response to Question 27.

(i) If so, what portions of *The Bell Curve* qualify as "hate speech?" Please provide quotations with page numbers for these portions.

Answer. See Response to Question 27.

(ii) If not, do Facebook's content policies prohibit a false claim that someone has engaged in "hate speech?"

Answer. See Response to Question 27.

(iii) What procedures or penalties does Facebook employ, if any, to discourage false claims that someone has engaged in hate speech?

Answer. See Response to Question 27.

Question 30. Are any portions of the Bible, quoted verbatim and with citation, subject to removal as:

(a) "Hate speech?" If so, please list the quotations and under which translation Facebook considers the quote "hate speech."

Answer. See Response to Question 27.

(b) Harassment? If so, please list the quotations and under which translation Facebook considers the quote harassment.

Answer. We do not tolerate harassment on Facebook because we want people to feel safe to engage and connect with their community. Our harassment policy applies to both public and private individuals and includes behavior like repeatedly contacting a single user despite that person's clear desire and action to prevent that contact and repeatedly contacting large numbers of people with no prior solicitation. It also applies to calls for death, serious disease or disability, or physical harm

aimed at an individual or group of individuals in a message thread. Context and intent matter, however, and we allow people to share and re-share posts if it is clear that something was shared in order to condemn or draw attention to harassment. The detailed guidelines our reviewers use to assess whether content violates our hate speech policies are available at *https://www.facebook.com/communitystandards/safety/harassment*.

We released our updated Community Standards—which reflect the guidelines our reviewers use to evaluate content that is reported to us—in order to better demonstrate where we draw lines on complex and continuously evolving issues. We also simultaneously launched an appeals process for content that has been removed for nudity/sexual activity, hate speech, and graphic violence. With this launch, we are giving people an opportunity to request review of our decisions and provide additional context that will help our team see a more complete picture as they review the post again. This type of feedback allows us to continue improving our systems and processes so we can prevent similar mistakes in the future.

Question 31. On April 19, 2018, the California State Assembly voted in favor of a bill, AB 2943, which would make it an "unlawful business practice" to engage in any transaction for a good or service that seeks "to change an individual's sexual orientation" The bill clarifies that this includes efforts to "change behaviors or gender expressions, or to eliminate or reduce sexual or romantic attractions or feelings toward individuals of the same sex." Multiple legal experts have observed that the bill's language, reasonably interpreted, could be read to outlaw the sale and purchase of books, such as the Bible, the Torah, and the Koran, which advocate for traditional sexual ethics.

(a) Yes or no: Does Facebook believe that books, such as the Bible, the Torah, and the Koran, which advocate for traditional sexual ethics, constitute hate speech?

Answer. See Response to Question 27.

(b) Yes or no: Does Facebook consider any part of the Bible, the Torah, and/or the Koran hate speech? If so, what parts of the Bible, the Torah, and/or the Koran qualify? Please provide quotations with page numbers for each part identified as hate speech.

Answer. See Response to Question 27.

(c) Yes or no: Does Facebook believe that the messages contained in books, such as the Bible, the Torah, and the Koran, which advocate for traditional sexual ethics (*i.e.* that sex should be had only within a marriage between one man and one woman), should be discouraged from public dissemination?

Answer. See Response to Question 27.

(d) Yes or no: Does Facebook agree with the California State Assembly that goods or services that seek to change behaviors or gender expressions deserve to be discouraged, muted, or banned?

Answer. See Response to Question 27.

(e) Yes or no: Does Facebook agree with the California State Assembly that goods or services that seek to eliminate or reduce sexual or romantic attractions or feelings toward individuals of the same sex deserve to be discouraged, muted, or banned?

Answer. See Response to Question 27.

(f) Yes or no: In the event AB 2943 is fully enacted into law, will Facebook comply with its provisions by removing, denying, downgrading, concealing, or otherwise censoring content and advertisements restricted by the bill? If so, does Facebook intend to remove, deny, downgrade, conceal, or otherwise censor content and advertisements that pertain to the Bible, the Torah, the Koran, and other books which advance traditional sexual ethics.

Answer. See Response to Question 27.

Question 32. If an individual posted any of the following statements, standing alone and not directed to any Facebook user in particular, would that statement violate Facebook's "hate speech" policy? To the extent that the decision would depend on additional facts, please describe whether the statement would prompt an investigation to determine whether it constitutes "hate speech," and whether the decision would involve algorithmic or human decision making.

(a) There are only two sexes or two genders, male and female.

(b) Bathroom segregation based on sex is similar to segregation based on race.

(c) God created man in his image, male and female.

(d) Gender is a social construct.

(e) A person's sex or gender are immutable characteristics.

(f) Sex reassignment surgery is a form of bodily mutilation.

(g) The abortion of an unborn child is murder.

(h) It should be a crime to perform or facilitate an abortion.

(i) It should be a crime to prevent someone from performing or obtaining an abortion.

(j) No person of faith should be required to assist a same-sex wedding by providing goods or services to a same-sex marrying couple.

(k) When an individual enters the marketplace, he gives up the right to choose whether to support a same-sex marriage.

(l) Islam is a religion of peace.

(m) Islam is a religion of war.

(n) All white people are inherently racist.

(o) All black people are inherently racist.

(p) Black lives matter.

(q) Blue lives matter.

(r) All lives matter.

(s) Donating to the NRA funds the murder of children, such as those slain in Parkland, Florida.

(t) Donating to Planned Parenthood funds the murder of children, such as those dismembered by Kermit Gosnell.

(u) Men should stop interrupting when women are talking.

(v) Women should stop interrupting when men are talking.

(w) DREAMers are Americans too and should be entitled to stay in this country.

(x) Illegal aliens need to be sent back.

(y) Religious beliefs are irrational and anti-science.

(z) Non-believers have no path to eternal salvation.

(aa) Affirmative Action policies discriminate on the basis of race and sex.

(bb) America is a "melting pot."

Answer. See Response to Question 27.

Question 33. Facebook states on its website that per its community standards, "organizations and people dedicated to promoting hatred" against protected groups are not allowed a presence on Facebook.

(a) What standards or policies does Facebook apply in determining whether a group violates this policy?

Answer. See Response to Question 15.

(b) Yes or no: Does Facebook contract with or in any way rely upon an outside party to determine what organizations and people are dedicated to promoting hatred against protected groups? If yes, please list the outside parties.

Answer. See Response to Question 15.

(c) Yes or no: Has Facebook ever referenced, used, consulted, or in any way relied upon the left-wing Southern Poverty Law Center's list of designated hate groups in order to determine whether an organization or individual was dedicated to promoting hatred against protected groups?

Answer. See Response to Question 15.

(d) Yes or no: Has Facebook ever denied an organization a presence on Facebook on account of the organization being dedicated to promoting hatred? If so, has Facebook ever reversed its decision to designate an organization a hate group under its community standards and reinstated the organization's privilege to post and have a presence on Facebook?

Answer. See Response to Question 15.

Question 34. One group on Facebook, "TERMINATE the Republican Party," has over 10,000 followers, one of which was James T. Hodgkinson. In June 2017, Hodgkinson opened fire on Republican members of Congress at a baseball practice, seriously wounding Rep. Steve Scalise, a congressional staffer, and two heroic police officers. Quotes from this group's posts and comments include that "These people are all the same, criminals, rapists, racists, Republicans;" that, about Rep. Patrick McHenry, "who gives birth to sorry pieces of s*** like him and allowed it to reach adulthood, truly needs a f*****g hammer to the head a few times;" and, referring to the President, "G*****n Russian roach traitor bastard . . . and his Republicanazi followers!" Each of these quotes took place long after Hodgkinson's shooting, though similar quotes are available from before it as well.

(a) Do these quotes constitute "hate speech?"

(i) If so, why have they not been removed?

(ii) If not, why do they not?

(b) If applied to Democrats, would the quotes above constitute "hate speech?"

(c) How has Facebook changed its platform in response to Hodgkinson's shooting? It has apparently not suspended or ended this group.

(d) Does it concern Facebook that such rhetoric is being used in a group which had an attempted political assassin as a member?

(e) Does Facebook permit threats of violence against the President?

(f) Does Facebook permit threats of violence against members of Congress?

(g) Does Facebook monitor its platforms for potential left-wing violence?

(i) If so, what is Facebook doing to ensure that shooters like Hodgkinson do not coordinate using Facebook?

(ii) If so, what is Facebook doing to ensure that shooters like Hodgskinson do not use Facebook to incite violence against Republicans or conservatives?

(iv) If not, why is Facebook not doing so given that its platform was integral to at least one attempted political assassination?

Answer. The shooting at the Congressional baseball practice was a horrendous act. As a designated mass shooting, any praise for that conduct or the shooter is against Facebook policies. We also do not allow any pages or accounts representing the shooter. If we are made aware of such comments, we would take them down.

We define hate speech as a direct attack on people based on what we call protected characteristics—race, ethnicity, national origin, religious affiliation, sexual orientation, sex, gender, gender identity, and serious disability or disease. We also provide some protections for immigration status. Political-party affiliation is not included in our list of protected characteristics. We define attack as violent or dehumanizing speech, statements of inferiority, and calls for exclusion or segregation. Our detailed hate speech policies are available at *https://www.facebook.com/communitystandards/objectionable_content/hate_speech*.

Our credible violence policies prohibit posting credible statements of intent to commit violence against any person, groups of people, or place (city or smaller). We assess credibility based upon the information available to us and generally consider statements credible if the following are present:

- A target (person, group of people, or place) and:
  - Bounty/demand for payment, or
  - Mention or image of specific weapon, or
  - Sales offer or ask to purchase weapon, or
  - Spelled-out address or named building, or
- A target and 2 or more of the following details (can be 2 of the same detail):
  - Location
  - Timing
  - Method

We also prohibit calls for violence, statements advocating violence, or aspirational or conditional statements of violence targeting public individuals, provided those statements are credible, as defined above. Any calls for violence against heads of state, including the United States President, violate our policies.

There are times someone might share something that would otherwise be considered hate speech but for non-hateful reasons, such as making a self-deprecating joke or quoting lyrics from a song. People often use satire and comedy to make a point about hate speech. In other cases, people may speak out against hatred by condemning someone else's use of offensive language, which requires repeating the original offense. This is something we allow, even though it might seem questionable since it means some people may encounter material disturbing to them.

Question 35. In July 2012, Governor Mike Huckabee praised Chick-fil-A because of its support for traditional marriage and called on Christians to support Chick-fil-A in its position by purchasing its products. Facebook temporarily removed Governor Huckabee's post from its service before reinstating it.

(a) Why was Governor Huckabee's post removed?

(b) What Facebook rule was Governor Huckabee's post thought to have violated before it was reinstated?

(c) Did Governor Huckabee's post violate Facebook's prohibition on "hate speech," either in 2012 or now?

(d) Does a post opposing the Supreme Court's decision in *Obergefell v. Hodges* violate Facebook's prohibition on "hate speech?"

(e) Does a post opposing legalized same-sex marriage violate Facebook's prohibition on "hate speech?"

(f) As of July 2012, had Facebook removed, downgraded, concealed, or otherwise censored any content created by a state Governor, member of the U.S. House of Representatives, member of the U.S. Senate, or the President on account of that individual's support for same-sex marriage? If so, please include the removed content including identifying information indicating its author.

(g) As of July 2012, had Facebook removed, downgraded, concealed, or otherwise censored any other content created by a state Governor, member of the U.S. House of Representatives, member of the U.S. Senate, or the President on account of that individual's opposition to same-sex marriage? If so, please include the removed content including identifying information indicating its author.

(h) Has, since July 2012, Facebook removed, downgraded, concealed, or otherwise censored any posts by a state Governor, member of the U.S. House of Representatives, member of the U.S. Senate, or the President on account of that individual's (or that content's) opposition to same-sex marriage? If so, please include the removed post identifying information indicating its author.

(i) Has, since July 2012, Facebook removed, downgraded, concealed, or otherwise censored any posts by a state Governor, member of the U.S. House of Representatives, member of the U.S. Senate, or the President on account of that individual's (or that content's) support for same-sex marriage? If so, please include the removed post identifying information indicating its author.

(j) Under what circumstances does Facebook remove, downgrade, conceal, or otherwise censor content that, though not threatening physical harm, promoting imminent physical self-harm, or advocating for terrorism, opposes same-sex marriage?

(k) Under what circumstances does Facebook remove, downgrade, conceal, or otherwise censor content that, though not threatening physical harm, promoting imminent physical self-harm, or advocating for terrorism, supports same-sex marriage?

Answer. In July 2012, our automated systems incorrectly removed an event page entitled "Chick-fil-A Appreciation Day." The page was restored within hours of coming to our attention. When we make mistakes on these important content decisions, we make every attempt to make it right as quickly as we can.

Our goal is to allow people to have as much expression as possible, including on the issue of same-sex marriage. We err on the side of allowing content, even when some find it objectionable, unless removing that content prevents a specific harm.

See also Response to Question 27.

Question 36. As described in the *Washington Post,* in October 2012, Facebook removed a post by a group called "Special Operations Speaks." The post said: "Obama called the SEALs and THEY got bin Laden. When the SEALs called Obama, they got denied," a reference to the failure of the Executive Branch to provide military support to Americans under assault, and later killed, in Benghazi. Facebook first warned the group that the post violated its rules and then subsequently removed the post as a violation of "Facebook's Statements of Rights and Responsibilities." Facebook further suspended Special Operations Speaks for 24 hours following the removal. Facebook later admitted error and permitted the content to remain on its platform.

(a) Why was Special Operations Speaks' post removed?

(b) What term of Facebook's then-extant 2012 Statement of Rights and Responsibilities was Special Operations Speaks' post thought to have violated before Facebook reversed its decision?

(c) Yes or no: Did any member of the Obama Administration, including any administrative agency then-directed by an executive official appointed by the Obama administration, contact Facebook to request that the post be removed?

(i) If so, whom?

(ii) What was Facebook's response?

(d) Yes or no: Did Facebook assure any government official or employee that this post would be removed? If so, whom?

(e) Did Special Operations Speaks' post violate Facebook's prohibition on "hate speech," either in 2012 or now?

(f) As of October 2012, had Facebook removed, downgraded, concealed, or otherwise censored any other content created by a political action committee on the basis of that content's disapproval of how the Obama administration handled the attack on U.S. diplomats and servicemen in Benghazi? If so, please include the removed content including identifying information about its author.

(g) As of October 2012, had Facebook removed, downgraded, concealed, or otherwise censored any content created by a political action committee on the basis of that content's approval of how the Obama administration handled the attack on U.S. diplomats and servicemen in Benghazi? If so, please include the removed content including identifying information about its author.

(h) Has, since October 2012, Facebook removed, downgraded, concealed, or otherwise censored any posts by a political action committee on the basis of that content's disapproval of how the Obama administration handled the attack on U.S. diplomats and servicemen in Benghazi? If so, please include the removed content including identifying information about its author.

(i) Has, since October 2012, Facebook removed, downgraded, concealed, or otherwise censored any posts by a political action committee on the basis of that content's disapproval of how the Obama administration handled the attack on U.S. diplomats and servicemen in Benghazi? If so, please include the removed content including identifying information about its author.

(j) Under what circumstances does Facebook remove, downgrade, conceal, or otherwise censor content that, though not threatening physical harm, promoting imminent physical self-harm, or advocating for terrorism, opposes the Obama Administration's handling of the attacks on U.S. diplomats and servicemen in Benghazi?

(k) Under what circumstances does Facebook remove, downgrade, conceal, or otherwise censor content that, though not threatening physical harm, promoting imminent physical self-harm, supports the Obama Administration's handling of the attacks on U.S. diplomats and servicemen in Benghazi?

Answer. In this particular case, we removed the content as a violation of our standards. The content was deleted for 29 hours. However, we realized that we made a mistake, and we restored the content and apologized for the error.

We define hate speech as a direct attack on people based on what we call protected characteristics—race, ethnicity, national origin, religious affiliation, sexual orientation, sex, gender, gender identity, and serious disability or disease. We also provide some protections for immigration status. We define attack as violent or dehumanizing speech, statements of inferiority, and calls for exclusion or segregation. Our detailed hate speech policies are available at *https://www.facebook.com/communitystandards/objectionable_content/hate_speech*.

Our Community Standards prohibit hate speech and celebrating graphic violence and allow people to use Facebook to raise awareness of and condemn violence. Drawing that line requires complex and nuanced judgments, and we carefully review reports that we receive from the public, media, civil society, and governments. We remove content that violates our policies, regardless of who posted the content.

Question 37. In September 2017, Facebook deemed the videos of two African American Trump supporters, known as Diamond and Silk, as "dangerous." In a company e-mail, Facebook stated that the decision was final and "not appealable in any way." Facebook then retracted this statement, explaining that the determination was inaccurate.

(a) What about Diamond and Silk did Facebook initially determine to be "dangerous?"

(b) What is Facebook's criteria for determining whether content that neither depicts nor advocates for violence as "dangerous?"

(c) Aside from the illustration of or advocacy for violence, under what conditions is the discussion of non-classified speech "dangerous?"

(d) Has Facebook implemented an appeals system by which users can challenge a determination of dangerousness?

(e) How often does Facebook retract these determinations?

(f) What is the internal review process for these types of determinations?

Answer. We mishandled communication with Diamond and Silk for months. Their frustration was understandable, and we apologized to them. The message they received on April 5, 2018 that characterized their Page as "dangerous" was incorrect and not reflective of the way we seek to communicate with our community and the people who run Pages on our platform.

As part of our commitment to continually improve our products and to minimize risks where human judgment is involved, we are making a number of changes:

- We have engaged an outside advisor, former Senator Jon Kyl, to advise the company on potential bias against conservative voices. We believe this external feedback will help us improve over time and ensure we can most effectively serve our diverse community.
- We continue to expand our list of outside organizations from across the political spectrum to provide feedback on potential changes to our content standards.
- We have made our detailed reviewer guidelines public to help people understand how and why we make decisions about the content that is and is not allowed on Facebook.
- We have launched an appeals process to enable people to contest content decisions with which they disagree. We recognize that we make enforcement errors on both sides of the equation—what to allow, and what to remove—and that our mistakes cause a great deal of concern for people, which is why we need to allow the option to request review of the decision and provide additional context that will help our team see the fuller picture as they review the post again. This type of feedback will allow us to continue improving our systems and processes so we can prevent similar mistakes in the future.

See also Response to Question 27.

Question 38. In October 2017, the social-media company Twitter refused to permit Representative Marsha Blackburn to pay to promote a campaign advertisement because Rep. Blackburn stated that she fought to stop the sale of children's body parts. Twitter's explanation was that Blackburn's critique of "the sale of baby body parts" was an "inflammatory statement" that Twitter refused to advertise.

(a) Does Representative Blackburn's campaign advertisement (available readily on the internet) violate Facebook's policies regarding acceptable advertisements?

(b) Does Representative Blackburn's campaign advertisement violate Facebook's policies against "hate speech?"

(c) Would the statement, standing alone, that Planned Parenthood sells baby body parts qualify as "hate speech?"

(d) Would Facebook censor or otherwise downgrade or make unavailable the statement that Planned Parenthood sells baby body parts for any other reason?

Answer. As Facebook indicated publicly in October 2017, Representative Blackburn's campaign advertisement, in which she mentioned "the sale of baby body parts" does not violate our Advertising Policies or our Community Standards.

We work to strike the right balance between enabling free expression around the globe and ensuring that our platform is safe. We currently define hate speech as anything that directly attacks people based on protected characteristics—race, ethnicity, national origin, religious affiliation, sexual orientation, sex, gender, gender identity, or serious disability or disease. We remove content that violates our policies, regardless of who posted the content, including the government.

Our policies allow content that may be controversial and at times even distasteful, but which does not cross the line into hate speech. This may include criticism of public figures, religions, professions, and political ideologies.

Question 39. Louis Farrakhan presently employs Facebook to reach numerous individuals. At present, he has over a million followers.

(a) On his Facebook page, Farrakhan links to an open letter of his which states: "We can now present to our people and the world a *true,* undeniable record of the relationship between Blacks and Jews from their own mouths and pens. These scholars, Rabbis and historians have given to us an undeniable record of Jewish anti-Black behavior, starting with the horror of the trans-Atlantic slave trade, plantation slavery, Jim Crow, sharecropping, the labor movement of the North and South, the unions and the misuse of our people that continues to this very moment."

(i) Does this statement violate Facebook's policies against "hate speech?"

(ii) If so, why has this post been permitted to remain?

(iii) If not, why not?

(b) On his Facebook page, Farrakhan links to a sermon in which he describes the "Synagogue of Satan" and its attempts to harm him.

(i) Is the term "Synagogue of Satan" a violation of Facebook's policies against "hate speech?"

(ii) If so, why has this post been permitted to remain?

(iii) If not, why not?

Answer. We are committed to designing our products to give all people a voice and foster the free flow of ideas and culture. That said, when something crosses the line into hate speech, it has no place on Facebook, and we are committed to removing it from our platform any time we become aware of it.

We define hate speech as a direct attack on people based on what we call protected characteristics—race, ethnicity, national origin, religious affiliation, sexual orientation, sex, gender, gender identity, and serious disability or disease. We also provide some protections for immigration status. We define attack as violent or dehumanizing speech, statements of inferiority, and calls for exclusion or segregation. The detailed guidelines our reviewers use to assess whether content violates our hate speech policies are available at *https://www.facebook.com/communitystandards/objectionable_content/hate_speech*.

Question 40. In June 2013, Facebook blocked the following post written by Fox News Radio's Todd Starnes for violating Facebook's community standards, "I'm about as politically incorrect as you can get. I'm wearing an NRA ball cap, eating a Chick-fil-A sandwich, reading a Paula Deen cookbook and sipping a 20-ounce sweet tea while sitting in my Cracker Barrel rocking chair with the Gather Vocal Band singing 'Jesus Saves' on the stereo and a Gideon's Bible in my pocket. Yes sir, I'm politically incorrect and happy as a June bug." Although Facebook ultimately reversed its decision, for several hours, Todd Starnes could not access either his fan or person page.

(a) Why was Todd Starnes' post removed?

(b) What Facebook rule was Todd Starnes' post thought to have violated before it was reinstated?

(c) Was any part of Starnes' statement "hate speech?"

(d) Was any part of Starnes' statement considered harassment?

(e) Yes or no: must posted content be "politically correct" to remain in accordance with Facebook's community standards?

(f) Is a statement that something is not "politically correct" a violation of Facebook's standards?

Answer. The page where Todd Starnes posted the content was not unpublished. He was the administrator that made the post, and the action was taken on his profile. He posted the content at around 2 a.m. on June 29, 2013, and it was restored shortly before 10 a.m. the same day. During that time, he did not lose his ability to access either his profile or his page, just the post itself. When we reinstated the post, we sent him an apology the same day.

Our policies apply equally to individuals and entities across the political spectrum. We are committed to designing our products to give all people a voice and foster the free flow of ideas and culture. That said, when something crosses the line into hate speech, it has no place on Facebook, and we are committed to removing it from our platform any time we become aware of it.

We recognize that our policies are only as good as the strength and accuracy of our enforcement—and our enforcement is not perfect. We make mistakes because our processes involve people, and people are not infallible. We are always working to improve.

When we're made aware of incorrect content removals, we review them with team members so as to prevent similar mistakes in the future. We also audit the accuracy of reviewer decisions on an ongoing basis to coach them and follow up on improving, where errors are being made.

We hope that our recent decision to publicize our detailed Community Standards—which reflect our internal reviewer guidelines—and the introduction of appeals will aid in this process. By providing more clarity on what is and isn't allowed on Facebook, we hope that people will better understand how our policies apply to them. Where people believe we have made a mistake, they can request review of our decisions.

Answer. See also Response to Question 44.

Question 41. How many individuals at Facebook have the ability to moderate, remove, downgrade, conceal, or otherwise censor content, ban, suspend, warn, or otherwise discipline users, or approve, price, review, or refuse advertisements on the platform? This question includes individuals with the power to alter search results and similar mechanisms that suggest additional content to users in order to to promote or demote content, whether individually or routinely through an algorithm or by altering any of the platform's search functions. (Please include all employees, independent contractors, or others with such ability at Facebook.)

(a) Into what divisions or groups are those individuals organized?

(b) Who are the individuals responsible for supervising these individuals as their conduct relates to American citizens, nationals, businesses, and groups?

(c) We understand from your April 10 testimony that Facebook has approximately 15,000 to 20,000 moderators. How many individuals have the responsibility to moderate, remove, downgrade, conceal, or otherwise censor content, ban, suspend, warn, or otherwise discipline users, or approve, price, review, or refuse advertisements as a primary or significant function of their role at Facebook? This question includes individuals with the power to alter search results and similar mechanisms that suggest additional content to users in order to to promote or demote content, whether individually or routinely through an algorithm or by altering any of the platform's search functions. (Going forward, we will refer to these individuals, with a primary or significant responsibility for reviewing content, users, or advertisements, as "moderators.")

(d) Who are the individuals responsible for supervising these moderators as their conduct relates to American citizens, nationals, businesses, and groups?

(e) How many moderators has Facebook had on its platform for each of the calendar years 2006 to 2018? Please provide approximations if exact numbers are impossible to obtain.

(f) How many moderators does Facebook intend to retain for the years 2019 and 2020?

(g) On average, how many pieces of content (*e.g.,* a Facebook post, an Instagram photo, and so on) does a moderator remove a day?

(h) On average, how many users does a moderator discipline a day?

(i) On average, how many advertisements does a moderator approve, disapprove, price, consult on, review, or refuse a day?

Answer. Our content reviewers respond to millions of reports each week from people all over the world.

Our community of users helps us by reporting accounts or content that may violate our policies. Our content review teams around the world—which grew by 3,000 people last year—work 24 hours a day and in dozens of languages to review these reports. By the end of 2018, we will have doubled the number of people working on safety and security as compared to the beginning of the year—to a total of 20,000.

To help the Facebook community better understand our efforts to enforce the Community Standards, we recently published a Community Standards Enforcement Preliminary Report (*https://transparency.facebook.com/community-standards-enforcement*) describing the amount and types of content we take action against, as well as the amount of content that we flag for review proactively.

We are also committed to getting better at enforcing our advertising policies. We review many ads proactively using automated and manual tools, and reactively when people hide, block, or mark ads as offensive. We are taking aggressive steps to strengthen both our automated and our manual review. We are also expanding our global ads review teams and investing more in machine learning to better understand when to flag and take down ads, such as ads that offer employment or credit opportunity while including or excluding multicultural advertising segments. Enforcement is never perfect, but we will get better at finding and removing improper ads.

As to the questions regarding ranking and algorithmic changes, see Response to Question 47.

Question 42. What percentage of Facebook's moderators:

(a) Self-identify or are registered as Democrats?

(b) Self-identify or are registered as Republicans?

(c) Would identify themselves as "liberal?"

(d) Would identify themselves as "conservative?"

(e) Have donated to:

(i) The Democratic Party?

(ii) A candidate running for office as a Democrat?

(iii) A cause primarily affiliated with or supported by the Democratic Party?

(iv) A cause primarily affiliated with or supported by liberal interest groups?

(v) A political action committee primarily advocating for the Democratic Party, Democratic candidates or office-holders, or causes primarily supported by the Democratic Party?

(vi) The Republican Party?

(vii) A candidate running for office as a Republican?

(viii) A cause primarily affiliated with or supported by the Republican Party?

(ix) A cause primarily affiliated with or supported by conservative interest groups?

(x) A political action committee primarily advocating for the Republican Party, Republican candidates or office-holders, or causes primarily supported by the Republican Party?

(f) Worked on or volunteered for a Democratic campaign?

(g) Worked on or volunteered for a Republican campaign?

(h) Worked on, interned for, or volunteered for a Democratic legislator, State or federal?

(i) Worked on, interned for, or volunteered for a Republican legislator, State or federal?

(j) Worked on or interned for a Democratic administration or candidate?

(k) Worked on or interned for a Republican administration or candidate?

Answer. We do not maintain statistics on these data points.

Question 43. What percentage of Facebook's employees:

(a) Self-identify or are registered as Democrats?

(b) Self-identify or are registered as Republicans?

(c) Self-identify as "liberal?"

(d) Self-identify as "conservative?"

(e) Have donated to:

(i) The Democratic National Committee, the Democratic Congressional Campaign Committee, or the Democratic Senatorial Campaign Committee?

(ii) A candidate running for office as a Democrat?

(iii) A cause primarily affiliated with or supported by the Democratic Party?

(iv) A cause primarily affiliated with or supported by liberal interest groups?

(v) A political action committee primarily advocating for the Democratic Party, Democratic candidates or office-holders, or causes primarily supported by the Democratic Party?

(vi) The Republican National Committee, the National Republican Senate Committee, or the National Republican Congressional Committee?

(vii) A candidate running for office as a Republican?

(viii) A cause primarily affiliated with or supported by the Republican Party?

(ix) A cause primarily affiliated with or supported by conservative interest groups?

(x) A political action committee primarily advocating for the Republican Party, Republican candidates or office-holders, or causes primarily supported by the Republican Party?

(f) Worked on, interned for, or volunteered for a Democratic candidate campaigning for elected office or an elected Democratic official or candidate?

(g) Worked on, interned for, or volunteered for a Republican campaigning for elected office or an elected Republican official or candidate?

(e) Have donated to:

(i) The Democratic National Committee, the Democratic Congressional Campaign Committee, or the Democratic Senatorial Campaign Committee?

(ii) A candidate running for office as a Democrat?

(iii) A cause primarily affiliated with or supported by the Democratic Party?

(iv) A cause primarily affiliated with or supported by liberal interest groups?

(v) A political action committee primarily advocating for the Democratic Party, Democratic candidates or office-holders, or causes primarily supported by the Democratic Party?

(vi) The Republican National Committee, the National Republican Senate Committee, or the National Republican Congressional Committee?

(vii) A candidate running for office as a Republican?

(viii) A cause primarily affiliated with or supported by the Republican Party?

(ix) A cause primarily affiliated with or supported by conservative interest groups?

(x) A political action committee primarily advocating for the Republican Party, Republican candidates or office-holders, or causes primarily supported by the Republican Party?

(f) Worked on, interned for, or volunteered for an elected Democratic official or candidate?

(g) Worked on, interned for, or volunteered for an elected Republican official or candidate?

Answer. We do not maintain statistics on these data points.

Question 45. What percentage of Facebook's executives:

(a) Self-identify or are registered as Democrats?

(b) Self-identify or are registered as Republicans?

(c) Self-identify as "liberal?"

(d) Self-identify as "conservative?"

(e) Have donated to:

(i) The Democratic National Committee, the Democratic Congressional Campaign Committee, or the Democratic Senatorial Campaign Committee?

(ii) A candidate running for office as a Democrat?

(iii) A cause primarily affiliated with or supported by the Democratic Party?

(iv) A cause primarily affiliated with or supported by liberal interest groups?

(v) A political action committee primarily advocating for the Democratic Party, Democratic candidates or office-holders, or causes primarily supported by the Democratic Party?

(vi) The Republican National Committee, the National Republican Senate Committee, or the National Republican Congressional Committee?

(vii) A candidate running for office as a Republican?

(viii) A cause primarily affiliated with or supported by the Republican Party?

(ix) A cause primarily affiliated with or supported by conservative interest groups?

(x) A political action committee primarily advocating for the Republican Party, Republican candidates or office-holders, or causes primarily supported by the Republican Party?

(f) Worked on, interned for, or volunteered for an elected Democratic official or candidate?

(g) Worked on, interned for, or volunteered for an elected Republican official or candidate?

Answer. We do not maintain statistics on these data points.

Question 46. How many employees has Facebook hired that previously worked for 501(c)(3) or 501(c)(4) nonprofits? Please list the names of the 501(c)(3) and 501(c)(4) organizations employees have previously worked for and the number of employees for each.

Answer. We do not maintain statistics on these data points.

Question 47. Based on your testimony, we understand that Facebook conducts many of its editorial and moderating decisions using one or more algorithms.

(a) What editorial and moderating functions do these algorithms undertake?

(b) List and describe the factors that the algorithm evaluates and considers.

(c) Describe what if any human oversight or auditing is in place to review the algorithm's functions.

(d) Do any of the factors in these algorithms associated with promoting, demoting, flagging, removing, suggesting, or otherwise altering the visibility of content correlate strongly (defined as meeting any generally accepted threshold for strong correlation using any generally accepted bivariate or multivariate analysis technique, including, but not limited to, chi-square, ANOVA, MANCOVA, Probit, Logit, regression, etc.) with any of the following traits (if so, please list which factor and its correlation):

(i) Self-identification with the Democratic Party?

(ii) Registration as a Democrat?

(iii) Self-identification as a liberal?

(iv) Self-identification with the Republican Party?

(v) Registration as a Republican?

(vi) Self-identification as a conservative?

(e) Do any of these factors correlate significantly (p greater than or equal to .05) with any of the following traits (if so, please list which factor and its correlation):

(i) Self-identification with the Democratic Party?

(ii) Registration as a Democrat?

(iii) Self-identification as a liberal?

(iv) Self-identification with the Republican Party?

(v) Registration as a Republican?

(vi) Self-identification as a conservative?

Answer. A user's News Feed is made up of stories from their friends, Pages they've chosen to follow and groups they've joined. Ranking is the process we use to organize all of those stories so that users can see the most relevant content at the top, every time they open Facebook. Ranking has four elements: the available inventory of stories; the signals, or data points that can inform ranking decisions; the predictions we make, including how likely we think a user is to comment on a story, share with a friend, etc.; and a relevancy score for each story.

News Feed considers thousands of signals to surface the content that's most relevant to each person who uses Facebook. Our employees don't determine the ranking of any specific piece of content. To help the community understand how News Feed works and how changes to News Feed affect their experience on Facebook, we publish a regularly-updated News Feed FYI blog (*https://newsroom.fb.com/news/category/inside-feed/*) where our team shares details of significant changes.

Question 48. What percentage of the individuals who design, code, implement, monitor, correct, or alter any of these algorithms:

(a) Self-identify as Democrats?

(b) Are registered as Democrats?

(c) Self-identify as liberal?

(d) Self-identify as Republicans?

(e) Are registered as Republicans?

(f) Self-identify as conservative?

Answer. We do not maintain statistics on these data points.

Question 49. In 2016, in response to complaints about "fake news" during the 2016 Presidential campaign and following President Trump's election, Facebook procured the services of specific "fact-checking" outlets in order to flag certain stories or sources as disputed, challenged, or incorrect. Earlier this year, it additionally changed one or more of the algorithms that recommend websites to users, such as users' news feeds.

(a) On what basis did Facebook select the fact-checking organizations that it enlisted to identify incorrect assertions of fact?

(b) Numerous sources have cited the presence of political bias in many "fact-checking" organizations; for example, according to one 2013 study by George Mason University's Center for Media and Public Affairs, the site Politifact.com—which Facebook employs to check facts on its platform—was between two and three times more likely to rate Republicans' claims as false (32 percent) than Democrats' claims (11 percent), and was between two and three times more likely to rate Democrats' statements as mostly or entirely true (54 percent) compared to Republicans' statements (18 percent). Indeed, the RealClearPolitics "Fact Check Review" notes that, in the last 120 days, approximately 1/6th of "facts" that Politifact.com claims to check aren't facts at all, but mere opinions.

(i) What steps does Facebook take to counteract liberal or left-wing bias by fact-checking outlets?

(ii) What steps does Facebook intend to take to bring political balance to its fact-checking review process?

(iii) What mechanisms for appealing a determination that a statement is false or otherwise disagreed-with does Facebook make available to entities that Politifact (or others) accuse(s) of lying?

(1) If none exist, what mechanisms does Facebook intend to make available?

(2) If none exist, to what extent will Facebook make its review of these claims publicly visible?

(iv) Has Facebook ever labeled claims or articles by any of the following entities as false? If so, please identify which claims and when.

(1) Huffington Post

(2) Salon

(3) Slate

(4) ThinkProgress

(5) Media Matters for America

(6) ShareBlue

(7) The Daily Kos

(8) Vice

(9) Vox

(10) TalkingPointsMemo

(v) Does Facebook consider the basis for a fact-checker's determination that something is "false" when choosing to label it as such? For example, as numerous media outlets have noted, some fact-checking outlets concede that the factual statement a public figure has made is true, but then condemn it for lacking "context" or spin favorable to a left-wing politician.

(1) If so, how does Facebook consider it?

(2) If not, does Facebook intend to do so in the future? And if so, how? If not, why not?

(c) When one of Facebook's fact-checkers determines that a claim is false, how does Facebook determine what material to refer a user to in response? Please list all such sources and any method relied on for determining their priority.

(d) Facebook's 2018 alteration of its algorithm has had a noted and outsized impact on traffic to conservative websites while not having a similar effect on liberal websites. At least one study by the *Western Journal* estimated liberal publishers' traffic from Facebook rose approximately 2 percent following the change, while conservative publishers' traffic declined approximately 14 percent.

(i) In what way(s) did Facebook change its content-screening or news-suggesting algorithms, or any other feature of its website which suggests content to users, in this 2018 instance?

(1) Were any components of these changes intended to have a differential impact on conservative outlets versus liberal ones?

(2) Were any components of these changes expected to have a differential impact on conservative outlets versus liberal ones?

(ii) Measured against pre-change traffic, how has the traffic of liberal publishers changed following this 2018 instance?

(iii) Measured against pre-change traffic, how has the traffic of conservative publishers changed following this 2018 instance?

(iv) Measured against pre-change traffic, how has this 2018 instance changed the traffic of the following publishers:

(1) The Washington Post

(2) The New York Times

(3) The Washington Times

(4) The New York Post

(5) The New York Daily News

(6) Fox News

(7) National Review

(8) The Daily Beast

(9) Huffington Post

(10) Buzzfeed

(11) Newsweek

(12) The Daily Wire

(13) Vice

(14) USA Today

(15) Salon

(16) Slate

(17) Vox
(18) The Daily Caller
(19) The Blaze
(20) PJ Media
(21) The Washington Free Beacon
(22) Reuters
(23) The Associated Press
(24) National Public Radio
(25) Bloomberg

(v) Does Facebook intend to do anything to reduce the differential effect on its recent algorithmic changes on conservative publishers?

(1) If so, what?
(2) If not, why not?

Answer. To reduce the spread of false news, one of the things we're doing is working with third-party fact checkers to let people know when they are sharing news stories (excluding satire and opinion) that have been disputed or debunked, and to limit the distribution of stories that have been flagged as misleading, sensational, or spammy. Third-party fact-checkers on Facebook are signatories to the non-partisan International Fact-Checking Network Code of Principles. Third-party fact-checkers investigate stories in a journalistic process meant to result in establishing the truth or falsity of the story.

In the United States, Facebook uses third-party fact-checking by the Associated Press, Factcheck.org, PolitiFact, Snopes, and the Weekly Standard Fact Check.

Publishers may reach out directly to the third-party fact-checking organizations if (1) they have corrected the rated content, or if (2) they believe the fact-checker's rating is inaccurate. To issue a correction, the publisher must correct the false content and clearly state that a correction was made directly on the story. To dispute a rating, the publisher must clearly indicate why the original rating was inaccurate. If a rating is successfully corrected or disputed, the demotion on the content will be lifted and the strike against the domain or Page will be removed. It may take a few days to see the distribution for the domain or Page recover. Additionally, any recovery will be affected by other false news strikes and related interventions (like demotions for clickbait). Corrections and disputes are processed at the fact-checker's discretion. Fact-checkers are asked to respond to requests in a reasonable time period—ideally one business day for a simple correction, and up to a few business days for more complex disputes.

We want Facebook to be a place where people can discover more news, information, and perspectives, and we are working to build products that help.

As to the questions regarding ranking and algorithmic changes, see Response to Question 47.

Question 50. Facebook's Help section explains that the posts that users see are influenced by their connections and activity on Facebook, including the number of comments, likes, and reactions a post receives and what kind of story it is. Some reporting suggests that Facebook's algorithm functions based on the content available (inventory), considerations about the content (signals), considerations about a person (predictions), and overall score.

(a) How do Facebook employees determine how informative a post is or which interactions create a more meaningful experience?

(b) Does a speaker's viewpoint determine in whole or part how informative or meaningful a post is?

(c) Does a speaker's partisan affiliation determine in whole or part how informative or meaningful a post is?

(d) Does a speaker's religious affiliation determine in whole or part how informative or meaningful a post is?

Answer. See Response to Question 47.

Question 51. Facebook is entitled to contribute money to Federal and State elections both as a function of the First Amendment as well as of Federal and State law. Including all of its subsidiaries, affiliates, as well as political action committees, partnerships, councils, groups, or entities organized with either a sole or significant purpose of electioneering, making political contributions to issue advocacy, candidates, or political parties, or of bundling or aggregating money for candidates or issue or party advocacy, whether disclosed by law or not, and during primary elections or general elections, how much money has Facebook contributed to:

(a) All federal, State, and local candidates for office from 2008 to present?

(b) All national party committees?

(i) Of that amount, how much was to:

(1) The Democratic National Committee?

(2) The Democratic Senatorial Campaign Committee?

(3) The Democratic Congressional Campaign Committee?

(4) The Republican National Committee?

(5) The National Republican Senate Committee?

(6) The National Republican Congressional Committee?

(c) All political action committees (or other groups outlined above in question 43) from 2008 to present?

(d) All issue-advocacy campaigns, including initiatives, referenda, ballot measures, and other direct-democracy or similar lawmaking measures?

(e) Candidates running for President:

(i) In 2008?

(1) How much of that money was to the Democratic candidate? (2) How much of that money was to the Republican candidate? (3) How much of that money was to other candidates?

(ii) In 2012?

(1) How much of that money was to the Democratic candidate?

(2) How much of that money was to the Republican candidate?

(3) How much of that money was to other candidates?

(iii) In 2016?

(1) How much of that money was to the Democratic candidate?

(2) How much of that money was to the Republican candidate?

(3) How much of that money was to other candidates?

(f) Candidates running for the U.S. Senate: (for special or off-year elections going forward, please group donation amounts with the next nearest cycle)

(i) In 2008?

(1) How much of that money was to Democratic candidates?

(2) How much of that money was to Republican candidates?

(3) How much of that money was to other candidates?

(ii) In 2010?

(1) How much of that money was to Democratic candidates?

(2) How much of that money was to Republican candidates?

(3) How much of that money was to other candidates?

(iii) In 2012?

(1) How much of that money was to Democratic candidates?

(2) How much of that money was to Republican candidates?

(3) How much of that money was to other candidates?

(iv) In 2014?

(1) How much of that money was to Democratic candidates?

(2) How much of that money was to Republican candidates?

(3) How much of that money was to other candidates?

(v) In 2016?

(1) How much of that money was to Democratic candidates?

(2) How much of that money was to Republican candidates?

(3) How much of that money was to other candidates?

(vi) In 2018?

(1) How much of that money was to Democratic candidates?

(2) How much of that money was to Republican candidates?

(3) How much of that money was to other candidates?

(g) Candidates running for the U.S. House of Representatives:

(i) In 2008?

(1) How much of that money was to Democratic candidates?
(2) How much of that money was to Republican candidates?
(3) How much of that money was to other candidates?

(ii) In 2010?

(1) How much of that money was to Democratic candidates?
(2) How much of that money was to Republican candidates?
(3) How much of that money was to other candidates?

(iii) In 2012?

(1) How much of that money was to Democratic candidates?
(2) How much of that money was to Republican candidates?
(3) How much of that money was to other candidates?

(iv) In 2014?

(1) How much of that money was to Democratic candidates?
(2) How much of that money was to Republican candidates?
(3) How much of that money was to other candidates?

(v) In 2016?

(1) How much of that money was to Democratic candidates?
(2) How much of that money was to Republican candidates?
(3) How much of that money was to other candidates?

(vi) In 2018?

(1) How much of that money was to Democratic candidates?
(2) How much of that money was to Republican candidates?
(3) How much of that money was to other candidates?

(h) Candidates running for Governor:

(i) In 2008?

(1) How much of that money was to Democratic candidates?
(2) How much of that money was to Republican candidates?
(3) How much of that money was to other candidates?

(ii) In 2010?

(1) How much of that money was to Democratic candidates?
(2) How much of that money was to Republican candidates?
(3) How much of that money was to other candidates?

(iii) In 2012?

(1) How much of that money was to Democratic candidates?
(2) How much of that money was to Republican candidates?
(3) How much of that money was to other candidates?

(iv) In 2014?

(1) How much of that money was to Democratic candidates?
(2) How much of that money was to Republican candidates?
(3) How much of that money was to other candidates?

(v) In 2016?

(1) How much of that money was to Democratic candidates?
(2) How much of that money was to Republican candidates?
(3) How much of that money was to other candidates?

(vi) In 2018?

(1) How much of that money was to Democratic candidates?
(2) How much of that money was to Republican candidates?

(3) How much of that money was to other candidates?

(i) Political action committees or other groups mentioned in question 43 that:

(i) Contribute 75 percent or more of their money to Democratic candidates for office?

(ii) Contribute 75 percent or more of their money to Republican candidates for office?

(iii) Identify as liberal, progressive, or otherwise left-wing?

(iv) Identify as conservative or right-wing?

Answer. Facebook complies with all political contribution reporting requirements, and such reports are publicly available. For more information on Facebook's contributions, please see *https://newsroom.fb.com/news/h/facebook-political-engagement/*.

Question 52. How much has Facebook donated, either in the form of money or services (including free or discounted advertising or more prominent placements within the platform via searches and other suggested-content mechanisms), to the following not-for-profit organizations (or their affiliates or subsidiaries) in the last 10 years? (Please separate answers into cash and non-cash components.)

(a) Planned Parenthood

(b) NARAL

(c) The Center for Reproductive Rights

(d) The National Right to Life Committee

(e) Americans United for Life

(f) Everytown for Gun Safety

(g) The Brady Campaign

(h) The National Rifle Association

(i) Gun Owners of America

(j) Human Rights Campaign

(k) Amnesty International

(l) Lambda Legal

(m) National Immigration Forum

(n) Federation

(o) GLAAD

(p) ACLU

(q) UnidosUS (formerly "La Raza" or the "National Council of La Raza")

(r) The Sierra Club

(s) Greenpeace

(t) The Heritage Foundation

(u) The Cato Institute

(v) The Institute for Justice

(w) Southern Poverty Law Center

(x) The Open Society Foundation(s)

(y) Americans for Prosperity

Answer. We partner with various domestic and international non-governmental organizations, which span the political and ideological spectrum. We provide our partners with technical expertise, sponsorships, advertising credits, and trainings, among other support. Our partnerships are crucial to our mission of building community. More information about our partnerships is available at *https://newsroom.fb.com/news/h/facebook-political-engagement/*.

Question 53. Facebook sells advertisements to political candidates and organizations. Multiple sources report that Facebook charged different rates to the Hillary Clinton and Donald Trump campaigns during the 2016 election. For the following questions, to the extent that geographic or local-market concerns significantly explain disparate rates between candidates, please explain how they do so and to what extent they do so, including calculations justifying that explanation.

(a) Did Facebook charge the two campaigns different rates?

(i) If so, on what basis?

(ii) If so, what rates did Facebook charge:

(1) The Clinton Campaign?

(2) The Trump Campaign?

(b) If these campaigns purchased advertising rates on Facebook or its platforms, what rates did Facebook charge each of the following campaigns?

(i) Barack Obama's 2008 campaign
(ii) John McCain's 2008 campaign
(iii) Barack Obama's 2012 campaign
(iv) Mitt Romney's 2012 campaign

(c) On average, and among campaigns that purchased advertisements, what rates did Facebook charge:

(i) Democrats running for Senate in 2008?
(ii) Republicans running for Senate in 2008?
(iii) Democrats running for the House of Representatives in 2008?
(iv) Republicans running for the House of Representatives in 2008?
(v) Democrats running for Governor in 2008?
(vi) Republicans running for Governor in 2008?
(vii) Democrats running in State or local legislative races in 2008?
(viii) Republicans running in State or local legislative races in 2008?
(ix) Democrats running for Senate in 2010?
(x) Republicans running for Senate in 2010?
(xi) Democrats running for the House of Representatives in 2010?
(xii) Republicans running for the House of Representatives in 2010?
(xiii) Democrats running for Governor in 2010?
(xiv) Republicans running for Governor in 2010?
(xv) Democrats running in State or local legislative races in 2010?
(xvi) Republicans running in State or local legislative races in 2010?
(xvii) Democrats running for Senate in 2012?
(xviii) Republicans running for Senate in 2012?
(xix) Democrats running for the House of Representatives in 2012?
(xx) Republicans running for the House of Representatives in 2012?
(xxi) Democrats running for Governor in 2012?
(xxii) Republicans running for Governor in 2012?
(xxiii) Democrats running in State or local legislative races in 2014?
(xxiv) Republicans running in State or local legislative races in 2014?
(xxv) Democrats running for Senate in 2014?
(xxvi) Republicans running for Senate in 2014?
(xxvii) Democrats running for the House of Representatives in 2014?
(xxviii) Republicans running for the House of Representatives in 2014?
(xxix) Democrats running for Governor in 2014?
(xxx) Republicans running for Governor in 2014?
(xxxi) Democrats running in State or local legislative races in 2014?
(xxxii) Republicans running in State or local legislative races in 2014?
(xxxiii) Democrats running in State or local legislative races in 2016?
(xxxiv) Republicans running in State or local legislative races in 2016?
(xxxv) Democrats running for Senate in 2016?
(xxxvi) Republicans running for Senate in 2016?
(xxxvii) Democrats running for the House of Representatives in 2016?
(xxxviii) Republicans running for the House of Representatives in 2016?
(xxxix) Democrats running for Governor in 2016?
(xl) Republicans running for Governor in 2016?
(xli) Democrats running in State or local legislative races in 2016?
(xlii) Republicans running in State or local legislative races in 2016?
(xliii) Democrats running in State or local legislative races in 2018?
(xliv) Republicans running in State or local legislative races in 2018?
(xlv) Democrats running for Senate in 2018?

(xlvi) Republicans running for Senate in 2018?

(xlvii) Democrats running for the House of Representatives in 2018?

(xlviii) Republicans running for the House of Representatives in 2018?

(xlix) Democrats running for Governor in 2018?

(l) Republicans running for Governor in 2018?

(li) Democrats running in State or local legislative races in 2018?

(lii) Republicans running in State or local legislative races in 2018?

(d) Yes or no: does Facebook consider partisan affiliation in deciding whether to sell advertisements to a political candidate, political action committee, or other organization purchasing political advertisements?

(e) Yes or no: does Facebook consider partisan affiliation in deciding at what rates to sell advertisements to a political candidate, political action committee, or other organization purchasing political advertisements?

(f) Yes or no: does Facebook consider the likelihood of a candidate's ultimate electoral success (via polls or otherwise) in deciding whether to sell advertisements to a political candidate?

(g) Yes or no: does Facebook consider the likelihood of a candidate's ultimate electoral success (via polls or otherwise) in deciding at what rates to sell advertisements to a political candidate?

Answer. Facebook offered identical support to both the Trump and Clinton campaigns, and had teams assigned to both. Everyone had access to the same tools, which are the same tools that every campaign is offered.

See also Response to Question 54.

Question 54. Please provide Facebook's advertising rates for each U.S. Senate and U.S. House election for which Facebook quoted or sold advertisements to one or more candidates for the years 2008, 2010, 2012, 2014, 2016, and 2018. For elections not falling in those years or special elections, please provide and group these rates with the next sequential election cycle. Where Facebook offered or sold advertising to multiple candidates within the same race, please pair those quotes or prices together along with party affiliation.

Answer. People can run ads on Facebook, Instagram and Audience Network on any budget. The exact cost associated with an ad being shown to someone is determined in Facebook's ad auction.

Question 55. Yes or no: has Facebook ever provided at no cost advertising to political candidates, campaign committees, political action committees or similar groups, or issue-advocacy groups or campaigns, whether through outright advertising or by altering search rankings, trending topics, content rankings, or the position of content within any suggested content mechanism?

(a) If so, please provide each instance in which Facebook has done so and indicate whether Facebook offered similar support to any other candidate or issue in that race or election.

(b) If so, please indicate whether Facebook coordinated with that campaign, candidate, or issue in doing so, or if Facebook acted unilaterally.

Answer. Political candidates, campaign committees, political action committees and similar groups, as well as issue advocacy groups and campaigns can set up Facebook Pages for free and post free content via those Pages, in the same way that any Page creator may. To run ads on Facebook, a form of payment must be provided. The algorithms that set content rankings are not designed to promote any candidate or party.

Question 56. Please list and describe all mandatory trainings that Facebook employees are required to undergo and the topics involved in each, including any trainings on sexual harassment, unconscious bias, racial privilege, and inclusivity.

Answer. At Facebook, we treat any allegations of harassment, discrimination, or retaliation with the utmost seriousness, and we have invested significant time and resources into developing our policies and processes. We have made our policies and processes available publicly—not because we think we have all the answers, but because we believe that the more companies are open about their policies, the more we can all learn from one another. Our internal policies on sexual harassment and bullying are available on our Facebook People Practices website (*http://peoplepractices.fb.com/*), along with details of our investigation process and tips and resources we have found helpful in preparing our Respectful Workplace internal trainings. Our philosophy on harassment, discrimination, and bullying is to go above and beyond what is required by law. Our policies prohibit intimidating, offensive, and sexual conduct even when that conduct might not meet the legal standard of

harassment. Even if it's legally acceptable, it's not the kind of behavior we want in our workplace. In developing our policies, we were guided by six basic principles:

- First, develop training that sets the standard for respectful behavior at work, so people understand what's expected of them right from the start. In addition to prescribing mandatory harassment training, we wrote our own unconscious bias training program at Facebook, which is also available publicly on our People Practices website. Our training includes Sustainable Equity, a three-day course in the U.S. about racial privilege and injustice, and Design for Inclusion, a multi-day course in the UK to educate on systemic inequity.
- Second, treat all claims—and the people who voice them—with seriousness, urgency, and respect. At Facebook, we make sure to have HR business partners available to support everyone on the team, not just senior leaders.
- Third, create an investigation process that protects employees from stigma or retaliation. Facebook has an investigations team made up of experienced HR professionals and lawyers trained to handle sensitive cases of sexual harassment and assault.
- Fourth, follow a process that is consistently applied in every case and is viewed by employees as providing fair procedures for both victims and those accused.
- Fifth, take swift and decisive action when it is determined that wrongdoing has occurred. We have a zero-tolerance policy, and that means that when we are able to determine that harassment has occurred, those responsible are fired. Unfortunately, in some cases investigations are inconclusive and come down to one person's word against another's. When we don't feel we can make a termination decision, we take other actions designed to help everyone feel safe, including changing people's roles and reporting lines.
- Sixth, make it clear that all employees are responsible for keeping the workplace safe—and anyone who is silent or looks the other way is complicit. There's no question that it is complicated and challenging to get this right. We are by no means perfect, and there will always be bad actors. Unlike law enforcement agencies, companies don't have access to forensic evidence and instead have to rely on reported conversations, written evidence, and the best judgment of investigators and legal experts. What we can do is be as transparent as possible, share best practices, and learn from one another—recognizing that policies will evolve as we gain experience. We don't have everything worked out at Facebook on these issues, but we will never stop striving to make sure we have a safe and respectful working environment for all our people.

We are also working to reduce unconscious bias. Our publicly available Managing Unconscious Bias class encourages our people to challenge and correct bias as soon as they see it—in others, and in themselves. We've also doubled down by adding two additional internal programs: Managing Inclusion, which trains managers to understand the issues that affect marginalized communities, and Be The Ally, which gives everyone the common language, tools, and space to practice supporting others.

Question 57. Please list and describe all optional recommended trainings that Facebook employees are required to undergo and the topics involved in each, including any trainings on sexual harassment, unconscious bias, racial privilege, and inclusivity.

Answer. See Response to Question 56.

Question 58. Do any of the materials Facebook uses in any of these trainings identify different preferences, values, goals, ideas, world-views, or abilities among individuals on the basis of the following? If so, please list each and include those materials.

(a) Race

(b) Sex

(c) Sexual orientation

(d) Place of origin

Answer. Diversity is core to our business at Facebook and we're committed to building and maintaining a workforce as diverse and inclusive as the people and communities we serve. We have developed and implemented programs and groups to help build a more diverse and inclusive company, and to better engage and support employees from diverse backgrounds. We have a number of Facebook Resource Groups (FBRGs) that are run by our internal communities from different backgrounds, such as Asians and Pacific Islanders, African-Americans, People with Disabilities, those of faith, Latinos/Hispanics, LGBTQ, Veterans, and women. These FBRGs provide members with support, foster understanding between all people, and

can coordinate programming to further support members. Examples of such programs include Women@ Leadership Day, Black@ Leadership Day, Latin@ Leadership Day, and Pride@ Leadership Day. Facebook also values and creates programming to support its Veterans and People with Disabilities through dedicated program managers and recruiters, mentoring programs and awareness campaigns to promote education and inclusion. These groups and programs are created to support and provide a more inclusive work experience for people from diverse backgrounds, with membership and participation open even to those who do not self-identify with these groups. For example, people who do not self-identify as Black are still members of Black@ and have attended Black@ Leadership Day, and there are male members of Women@ and men can attend Women@ Leadership Day. Facebook is also an Equal Opportunity Employer.

Question 59. Facebook acknowledges that it is located in a very liberal part of the country, and has suggested that it understands that many of its employees as well as the surrounding community share a particular (very liberal) culture.

(a) Does Facebook have any training specifically aimed at discouraging political, ideological, or partisan bias in decision-making by its employees?

(b) Does Facebook have any training specifically aimed at discouraging political, ideological, or partisan bias in hiring, retention, promotion, and firing of its employees?

(c) Does Facebook have any training specifically aimed at discouraging political, ideological, or partisan bias in the monitoring and supervision of content, users, or advertisements on each of its platforms?

Answer. Our Community Standards are global and all reviewers use the same guidelines when making decisions.

They undergo extensive training when they join and, thereafter, are regularly trained and tested with specific examples on how to uphold the Community Standards and take the correct action on a piece of content. This training includes when policies are clarified, or as they evolve.

We seek to write actionable policies that clearly distinguish between violating and non-violating content and we seek to make the decision making process for reviewers as objective as possible.

Our reviewers are not working in an empty room. There are quality control mechanisms as well as management on site to help or seek guidance from if needed. When a reviewer isn't clear on the action to take based on the Community Standards, they can pass the content decision to another team for review.

We also audit the accuracy of reviewer decisions on an ongoing basis to coach them and follow up on improving, where errors are being made.

When we're made aware of incorrect content removals, we review them with our Community Operations team so as to prevent similar mistakes in the future.

We recently introduced the right to appeal our decisions on individual posts so users can ask for a second opinion when they think we've made a mistake. As a first step, we are launching appeals for posts that were removed for nudity/sexual activity, hate speech or graphic violence. We are working to extend this process further, by supporting more violation types, giving people the opportunity to provide more context that could help us make the right decision, and making appeals available not just for content that was taken down, but also for content that was reported and left up. We believe giving people a voice in the process is another essential component of building a fair system.

Question 60. Please list the names of any third-party organizations or vendors that Facebook uses to facilitate its trainings.

Answer. We have a comprehensive training program that includes many hours of live instructor-led training, as well as hands-on practice for all of our reviewers.

All training materials are created in partnership with our policy team and in-market specialists or native speakers from the region.

After starting, reviewers are regularly trained and tested with specific examples on how to uphold the Community Standards and take the correct action on a report. Additional training happens continuously and when policies are clarified, or as they evolve.

Question 61. In the last five years, how many discrimination complaints has Facebook received from Christians? Please indicate how these complaints were resolved.

Answer. Decisions about content are made based on whether content violates our Community Standards. A user's personal characteristics do not influence the decisions we make, and Facebook does not track the religious beliefs or other personal characteristics of complainants.

Question 62. Yes or no: Does Facebook offer any compensation, amenities, trainings, or similar services to its employees on account of their race, sex, sexual orientation, or religious affiliation? If so, please list each and whether all other races, sexes, etc. are provided the same compensation, amenity, etc.

Answer. See Response to Question 58.

Question 63. In August 2017, Google fired James Damore for violating its code of conduct after Damore submitted an internal memo criticizing the company's hiring practices and arguing that the company's political bias created a negative work environment.

(a) Yes or no: Does Facebook agree with Google's decision to fire James Damore?

(b) Would an individual at Facebook have been fired for publishing a memorandum like Damore's? Assume no previous negative disciplinary history.

(c) Does Facebook permit employees to believe that some portion of the career differences between men and women are the result of differing choices between the sexes?

(i) Would a Facebook employee be disciplined for mentioning that opinion in a conversation to a willing participant?

(ii) Would a Facebook employee be disciplined for mentioning that opinion on his or her Facebook account?

(d) Does Facebook permit employees to criticize its "diversity" efforts as being racist against whites or sexist against men?

(i) Would a Facebook employee be disciplined for mentioning that opinion in a conversation to a willing participant?

(ii) Would a Facebook employee be disciplined for mentioning that opinion on his or her Facebook account?

Answer. We try to run our company in a way where people can express different opinions internally. We are not in a position to comment on the personnel decisions of another company or to engage in speculation about how we might respond in particular hypothetical circumstances.

Question 64. In October 2017, Prager University filed suit against Google and Youtube, alleging that the two companies illegally discriminated against Prager University because of its conservative political perspective. As evidence, Prager University pointed to the dozens of educational videos that Youtube either put in "restricted mode" or demonetized.

(a) Yes or no: Does Facebook agree with YouTube/Google's decision to restrict the following Prager University video, and if so, why?

(i) The World's Most Persecuted Minority: Christians?

(ii) Israel's Legal Founding?

(iii) Are the Police Racist?

(iv) Why Did America Fight the Korean War?

(v) What Should We Do About Guns?

(vi) Why America Must Lead?

(vii) The Most Important Question About Abortion?

(b) Yes or no: Does Facebook agree with YouTube/Google's decision to demonetize the following Prager University video, and if so, why?

(i) Are The Police Racist?

(ii) Israel's Legal Founding

(iii) The Most Important Question About Abortion?

(iv) Who's More Pro-Choice: Europe or America?

(v) Why Do People Become Islamic Extremists?

(vi) Is the Death Penalty Ever Moral?

(vii) Why Isn't Communism as Hated as Nazism?

(viii) Radical Islam: The Most Dangerous Ideology?

(ix) Is Islam a Religion of Peace?

Answer. See Response to Question 27.

Question 65. Recently, Jack Dorsey, Twitter's CEO, praised an article by two Democrats calling for a "new civil war" against the Republican Party, in which "the entire Republican Party, and the entire conservative movement that has controlled

it for the past four decades" will be given a "final takedown that will cast them out" to the "political wilderness" "for a generation or two."

(a) Does you agree with the premise of this article? It is located here: *https://medium.com/s/state-of-the-future/the-great-lesson-of-california-in-americas-new-civil-war-e52e2861f30*

(b) Do you or Facebook believe it is appropriate for its platform or company to call for a "new civil war?"

(c) Do you or Facebook believe it is appropriate for its platform or company to call for an end to one of the Nation's two major political parties?

(d) Do you or Facebook believe it is appropriate for its platform or company to call for an end to the conservative movement?

(e) Do you or Facebook condemn Twitter for calling for an end to the Republican Party?

(f) Do you or Facebook condemn Twitter for calling for an end to the conservative movement?

(g) Do you or Facebook condemn Twitter for calling for a new American civil war?

Answer. We are not in a position to comment on the decisions of another company or on another company's executive's statements about a news articles.

We are committed to designing our products to give all people a voice and foster the free flow of ideas and culture. That said, when something crosses the line into hate speech, it has no place on Facebook, and we are committed to removing it from our platform any time we become aware of it.

Question 66. Does Facebook collect information regarding its users':

(a) Usage of non-Facebook apps?

(b) E-mail?

(c) Audio or ambient sound?

(d) Telephone usage?

(e) Text messaging?

(f) iMessaging?

(g) Physical location when the user is not using the Facebook app?

(h) Spending?

Answer. As explained in our Data Policy, we collect three basic categories of data about people:

(1) data about things people do and share (and who they connect with) on our services,

(2) data about the devices people use to access our services, and

(3) data we receive from partners, including the websites and apps that use our business tools.

As far as the amount of data we collect about people, the answer depends on the person. People who have only recently signed up for Facebook have usually shared only a few things—such as name, contact information, age, and gender. Over time, as people use our products, we receive more data from them, and this data helps us provide more relevant content and services. That data will fall into the categories noted above, but the specific data we receive will, in large part, depend on how the person chooses to use Facebook. For example, some people use Facebook to share photos, so we receive and store photos for those people. Some people enjoy watching videos on Facebook; when they do, we receive information about the video they watched, and we can use that information to help show other videos in their News Feeds. Other people seldom or never watch videos, so we do not receive the same kind of information from them, and their News Feeds are likely to feature fewer videos.

The data we have about people also depends on how they have used our controls. For example, people who share photos can easily delete those photos. The same is true of any other kind of content that people post on our services. Through Facebook's Activity Log tool, people can also control the information about their engagement—*i.e.,* their likes, shares and comments—with other people's posts. The use of these controls of course affects the data we have about people.

Question 67. Does Facebook give its users the opportunity to opt out of Facebook collecting its users' data while still using the service?

Answer. The Ad Preferences tool on Facebook shows people the advertisers whose ads the user might be seeing because they visited the advertisers' sites or apps. The person can remove any of these advertisers to stop seeing their ads.

In addition, the person can opt out of these types of ads entirely—so he or she never sees those ads on Facebook based on information we have received from other websites and apps.

We've also announced plans to build Clear History, a feature that will enable people to see the websites and apps that send us information when they use them, delete this information from their accounts, and turn off our ability to store it associated with their accounts going forward.

Apps and websites that use features such as the Like button or Facebook Analytics send us information to make their content and ads better. We also use this information to make user experience on Facebook better.

If a user clears his or her history or uses the new setting, we'll remove identifying information so a history of the websites and apps the user used won't be associated with the user's account. We'll still provide apps and websites with aggregated analytics—for example, we can build reports when we're sent this information so we can tell developers if their apps are more popular with men or women in a certain age group. We can do this without storing the information in a way that's associated with the user's account, and as always, we don't tell advertisers who users are.

It will take a few months to build Clear History. We'll work with privacy advocates, academics, policymakers and regulators to get their input on our approach, including how we plan to remove identifying information and the rare cases where we need information for security purposes. We've already started a series of roundtables in cities around the world, and heard specific demands for controls like these at a session we held at our headquarters. We're looking forward to doing more.

Question 68. Yes or no: In preparation for the April 10, 2018 hearing, did Facebook, employees of Facebook, or independent contractors hired by Facebook examine the personal Facebook pages of the U.S. Senators scheduled to take part in the hearing?

(a) If so, please identify the Facebook pages visited and the information sought.

(b) If so, please identify the individuals who sought such information and what information they obtained.

(c) If so, please identify all individuals who possessed or reviewed that information.

Answer. While Facebook employees regularly look at the public pages of members of Congress to track the issues that are important to them, we are confident that no employees accessed any private data on personal profiles to prepare for the hearing or the questions for the record.

Question 69. Yes or no: In preparation for the April 10, 2018 hearing, did Facebook, employees of Facebook, or independent contractors hired by Facebook examine the personal Facebook pages of U.S. Senators' family members?

(a) If so, please identify the Facebook pages visited and the information sought.

(b) If so, please identify the individuals who sought such information and what information they obtained.

(c) If so, please identify all individuals who possessed or reviewed that information.

Answer. See Response to Question 68.

Question 70. Yes or no: In preparation for the April 10, 2018 hearing, did Facebook, employees of Facebook, or independent contractors hired by Facebook examine the personal Facebook pages of any Senate employees?

(a) If so, please identify the Facebook pages visited and the information sought.

(b) If so, please identify the individuals who sought such information and what information they obtained.

(c) If so, please identify all individuals who possessed or reviewed that information.

Answer. See Response to Question 68.

Question 71. Yes or no: In responding to these or any other questions for the record arising from the April 10, 2018 hearing, did Facebook, employees of Facebook, or independent contractors hired by Facebook examine the personal Facebook pages of the U.S. Senators scheduled to take part in the hearing?

(a) If so, please identify the Facebook pages visited and the information sought.

(b) If so, please identify the individuals who sought such information and what information they obtained.

(c) If so, please identify all individuals who possessed or reviewed that information.

Answer. See Response to Question 68.

Question 72. Yes or no: In responding to these or any other questions for the record arising from the April 10, 2018 hearing, did Facebook, employees of Facebook, or independent contractors hired by Facebook examine the personal Facebook pages of U.S. Senators' family members?

(a) If so, please identify the Facebook pages visited and the information sought.

(b) If so, please identify the individuals who sought such information and what information they obtained.

(c) If so, please identify all individuals who possessed or reviewed that information.

Answer. See Response to Question 68.

Question 73. Yes or no: In responding to these or any other questions for the record arising from the April 10, 2018 hearing, did Facebook, employees of Facebook, or independent contractors hired by Facebook examine the personal Facebook pages of U.S. Senate employees?

(a) If so, please identify the Facebook pages visited and the information sought.

(b) If so, please identify the individuals who sought such information and what information they obtained.

(c) If so, please identify all individuals who possessed or reviewed that information.

Answer. See Response to Question 68.

Question 74. Yes or no: Does Facebook collect data on individuals who are not registered Facebook users?

(a) If so, does Facebook use this data as part of the advertising products it sells?

(b) If so, does Facebook share or has Facebook ever shared this data with third parties?

Answer. Facebook does not create profiles for people who do not hold Facebook accounts.

When people visit apps or websites that feature our technologies—like the Facebook Like or Comment button—our servers automatically log (i) standard browser or app records of the fact that a particular device or user visited the website or app (this connection to Facebook's servers occurs automatically when a person visits a website or app that contains our technologies, such as a Like button, and is an inherent function of Internet design); and (ii) any additional information the publisher of the app or website chooses to share with Facebook about the person's activities on that site (such as the fact that a purchase was made on the site). This is a standard feature of the Internet, and most websites and apps share this same information with multiple different third-parties whenever people visit their website or app. For example, the Senate Commerce Committee's website shares information with Google and its affiliate DoubleClick and with the analytics company Webtrends. This means that, when a person visits the Committee's website, it sends browser information about their visit to each one of those third parties. More information about how this works is available at *https://newsroom.fb.com/news/2018/04/data-off-facebook/*.

When the person visiting a website featuring Facebook's tools is not a registered Facebook user, Facebook does not have information identifying that individual, and it does not create profiles for this individual.

We use the browser and app logs that apps and websites send to us—described above—in the following ways for non-Facebook users. First, these logs are critical to protecting the security of Facebook and to detecting or preventing fake account access. For example, if a browser has visited hundreds of sites in the last five minutes, that's a sign the device might be a bot, which would be an important signal of a potentially inauthentic account if that browser then attempted to register for an account. Second, we aggregate those logs to provide summaries and insights to websites and apps about how many people visit or use their product, or use specific features like our Like button—but without providing any information about a specific person. We do not create profiles for non-Facebook users, nor do we use browser and app logs for non-Facebook users to show targeted ads from our advertisers to them or otherwise seek to personalize the content they see. However, we may take the opportunity to show a general ad that is unrelated to the attributes of the person or an ad encouraging the non-user to sign up for Facebook.

Question 75. To the extent that Facebook collects and uses data from individuals who are not registered Facebook users, has Facebook gained consent from those individuals to collect and use their personal data?

Answer. Facebook does not create profiles about or track web or app browsing history for people who are not registered users of Facebook.

Question 76. To the extent that Facebook collects and uses data from individuals who are registered Facebook users, has Facebook obtained those individuals' informed consent on an opt-in basis prior to the acquisition of that data?

(a) If so, please provide the basis for concluding that data was acquired on an informed consent basis.

(b) If so, please provide the basis for concluding that users opted-in to Facebook's collection and commercialization of their data.

Answer. All users must expressly consent to Facebook's Terms and Data Policy when registering for Facebook. The Data Policy explains the kinds of information we collect, how we use this information, how we share this information, and how users can manage and delete information. After joining Facebook, people are presented with the opportunity to consent to additional data collection and uses, such as the use of location or the users' address book on their mobile device.

In response to your specific questions, depending on which Services a person uses, we collect different kinds of information from or about them. This is described in our Data Policy:

Things users and others do and provide.

- *Information and content users provide.* We collect the content, communications and other information users provide when they use our Products, including when they sign up for an account, create or share content, and message or communicate with others. This can include information in or about the content they provide (like metadata), such as the location of a photo or the date a file was created. It can also include what they see through features we provide, such as our camera, so they can do things like suggest masks and filters that users might like, or give them tips on using camera formats. Our systems automatically process content and communications users and others provide to analyze context and what's in them for the purposes described below.
  - *Data with special protections.* Users can choose to provide information in their Facebook profile fields or Life Events about their religious views, political views, who they are "interested in," or their health. This and other information (such as racial or ethnic origin, philosophical beliefs or trade union membership) could be subject to special protections under the laws of a user's country.
- *Networks and connections.* We collect information about the people, Pages, accounts, hashtags, and groups users are connected to and how users interact with them across our Products, such as people users communicate with the most or groups they are part of. We also collect contact information if users choose to upload, sync or import it from a device (such as an address book or call log or SMS log history), which we use for things like helping users and others find people they may know and for the other purposes listed below.
- *Users' usage.* We collect information about how users use our Products, such as the types of content they view or engage with; the features they use; the actions they take; the people or accounts they interact with; and the time, frequency and duration of their activities. For example, we log when users are using and have last used our Products, and what posts, videos and other content users view on our Products. We also collect information about how users use features like our camera.
- *Information about transactions made on our Products.* If users use our Products for purchases or other financial transactions (such as when they make a purchase in a game or make a donation), we collect information about the purchase or transaction. This includes payment information, such as their credit or debit card number and other card information; other account and authentication information; and billing, shipping and contact details.
- *Things others do and information they provide about users.* We also receive and analyze content, communications and information that other people provide when they use our Products. This can include information about users, such as when others share or comment on a photo of them, send a message to them, or upload, sync or import their contact information.

Device Information

- As described below, we collect information from and about the computers, phones, connected TVs and other web-connected devices users use that integrate with our Products, and we combine this information across different devices users use. For example, we use information collected about users' use of our Products on their phone to better personalize the content (including ads) or fea-

tures they see when they use our Products on another device, such as their laptop or tablet, or to measure whether they took an action in response to an ad we showed them on their phone on a different device.

- Information we obtain from these devices includes:
  - *Device attributes:* information such as the operating system, hardware and software versions, battery level, signal strength, available storage space, browser type, app and file names and types, and plugins.
  - *Device operations:* information about operations and behaviors performed on the device, such as whether a window is foregrounded or backgrounded, or mouse movements (which can help distinguish humans from bots).
  - *Identifiers:* unique identifiers, device IDs, and other identifiers, such as from games, apps or accounts users use, and Family Device IDs (or other identifiers unique to Facebook Company Products associated with the same device or account).
  - *Device signals:* Bluetooth signals, and information about nearby Wi-Fi access points, beacons, and cell towers.
  - *Data from device settings:* information users allow us to receive through device settings they turn on, such as access to their GPS location, camera, or photos.
  - *Network and connections:* information such as the name of users' mobile operator or ISP, language, time zone, mobile phone number, IP address, connection speed and, in some cases, information about other devices that are nearby or on their network, so we can do things like help users stream a video from their phone to their TV.
  - *Cookie data:* data from cookies stored on a user's device, including cookie IDs and settings. Learn more about how we use cookies in the Facebook Cookies Policy (*https://www.facebook.com/policies/cookies/*) and Instagram Cookies Policy (*https://www.instagram.com/legal/cookies/*)

Information from partners.

- Advertisers, app developers, and publishers can send us information through Facebook Business Tools they use, including our social plug-ins (such as the Like button), Facebook Login, our APIs and SDKs, or the Facebook pixel. These partners provide information about users' activities off Facebook—including information about their device, websites they visit, purchases they make, the ads they see, and how they use their services—whether or not they have a Facebook account or are logged into Facebook. For example, a game developer could use our API to tell us what games a user plays, or a business could tell us about a purchase a user made in its store. We also receive information about users' online and offline actions and purchases from third-party data providers who have the rights to provide us with users' information.
- Partners receive users' data when users visit or use their services or through third parties they work with. We require each of these partners to have lawful rights to collect, use and share users' data before providing any data to us.

Question 77. Yes or no: Does Facebook give non-Facebook users a reasonable opportunity to learn what information has been collected about them by Facebook? If yes, please describe how.

Answer. Yes. If a person doesn't have a Facebook account but believes Facebook may have information about them, they can contact us to request a copy of their information. A contact form is available at *https://www.facebook.com/help/contact/180237885820953*.

However, Facebook does not create profiles about or track web or app browser behavior of non-users.

Question 78. During the April 10, 2018 joint committee hearing, you stated, "Every piece of content that you share on Facebook, you own and you have complete control over who sees it and—and how you share it, and you can remove it at any time." To corroborate that statement, you cited multiple mechanisms provided by Facebook that allow users to locate, edit, download, and delete information collected about them by Facebook.

(a) Yes or no: Does Facebook offer non-Facebook users the same opportunities to control and edit any data collected about them by Facebook?

Answer. A user owns the information they share on Facebook. This means they decide what they share and who they share it with on Facebook, and they can change their mind. We believe everyone deserves good privacy controls. We require websites and apps who use our tools to tell users they're collecting and sharing their

information with us, and to get users' permission to do so. However, non-Facebook users cannot post content on Facebook. Accordingly, there are not corresponding controls for non-Facebook users.

(b) Facebook's "Privacy Basics" on deleting posts states "Hiding lets you keep your post but no one else will be able to see it when they view your Timeline. Note that it might still show up in search results and other places on Facebook."

(i) How does an individual have "complete control" over their data if a post that has been hidden still shows up "in search results and other places on Facebook?"

Answer. A user can delete any post they have made. If they do so, it will not appear in search results and in other places on Facebook. The language you refer to appears in a feature that allows people to hide—not delete—content from their personal timeline. That is, a person can choose to delete a post that they have made from Facebook entirely, or they can choose to hide a post from their timeline even though it may be visible in other places on Facebook.

(ii) Does Facebook give users an opportunity delete their content or information from these "other places" or search results?

Answer. Yes. See Response to Question 78(b)(i).

(iii) Does Facebook give non-users an opportunity to delete content containing or relating to them from these "other places" or search results?

Answer. Since this passage refers to content created by Facebook users and whether it's visible on their timeline, this does not apply to non-users. See the responses to the sub-questions above and below.

(c) If a Facebook user deletes a post will it show up in search results and other places on Facebook? If so, please describe the other places on Facebook in which a deleted post may appear.

Answer. In general, when a user deletes their account, we delete things they have posted, such as their photos and status updates, and they won't be able to recover that information later. (Information that others have shared about them isn't part of their account and won't be deleted.)

There are some limited exceptions to these policies: For instance, information can be accessed and preserved for an extended period when it is the subject of a legal request or obligation, governmental investigation, or investigations of possible violations of our terms or policies, or otherwise to prevent harm. We also retain information from accounts disabled for terms violations for at least a year to prevent repeat abuse or other term violations.

(d) If a Facebook user deletes his account, will any of his data show up in search results and other places on Facebook?

Answer. See Response to Question 78(c).

(i) Will Facebook retain any of his data for any purpose? If so, please describe what data and for what purposes.

Answer. See Response to Question 78(c).

Question 79. Yes or no: does Facebook employ facial-recognition technology?

(a) If so, does Facebook collect user data using facial-recognition technology?

(b) If so, does Facebook collect data on individuals who are not registered Facebook users using facial-recognition technology?

(c) If yes, does Facebook allow third-parties access to its facial-recognition technology or related information obtained as a result of the technology?

(d) If yes, does Facebook allow government entities access to its facial recognition technology and/or the information obtained as a result of the technology?

(e) To the extent that Facebook uses facial-recognition technology, what policies and procedures does Facebook have to safeguard information and data collected using that technology?

(f) Does Facebook offer individuals, whether registered users or not, any opportunity to not be subject to facial-recognition technology or to have data collected using facial-recognition technology deleted?

(g) Yes or no: Will Facebook commit to not using its facial-recognition technology to assemble data on individuals who have never consented to being part of Facebook?

Answer. Facebook uses facial recognition technology to provide people with products and features that enhance online experiences for Facebook users while giving them control over this technology. Facebook's facial recognition technology helps people tag their friends in photos; gives people an easier and faster way to privately share their photos with friends; helps people with visual impairments by generating descriptions of photos that people using screen readers can hear as they browse

Facebook; lets people know when a photo or video of them has been uploaded to Facebook, even if they are not tagged; and helps prevent people from impersonating other Facebook users.

Facial recognition technology uses machine-learning algorithms to analyze the pixels in photos and videos in which a user is tagged, and the photo used by the person as his or her profile picture, and generates a unique number called a template. When a photo or video is uploaded to Facebook, Facebook uses the template to attempt to identify someone by determining whether there are any faces in that content, and analyzing the portion of the image in which the face appears to compare it against certain Facebook users depending on the purpose for which facial recognition is being performed.

Facebook has not shared and does not have plans to share or make available to any third party its facial recognition templates. Moreover, these templates do not provide meaningful information on their own; they can be used to identify a person only in conjunction with Facebook's software. They could not be reverse-engineered to recreate someone's face.

Facebook designed its facial-recognition technology and the applications that use it with privacy considerations in mind and incorporated various safeguards and controls that protect both (1) users' ability to control the collection, use, and disclosure of their personal information, and (2) the security of that personal information.

Facebook gives users control over whether Facebook uses facial recognition to recognize them in photos and videos. That control is exercised through users' privacy settings. If a user chooses to turn facial recognition off, Facebook does not create a template for that person or deletes any template it has previously created. Facebook will then be unable to recognize that person in any photos or videos that are uploaded to the service. Facebook also deletes templates of people who delete their Facebook accounts. Additionally, Facebook does not maintain templates for users who have no photos tagged of themselves and do not have a profile photo that is capable of being used to generate a face signature or template (*e.g.,* where a user has no profile photo, where a user's profile photo does not contain a human face, or where a user's profile photo contains multiple untagged faces).

We inform people about our use of facial-recognition technology through the Data Policy, Help Center, posts on Facebook, and direct user notifications. Facebook users are told that they can opt out of facial recognition at any time—in which case Facebook will delete their template and will no longer use facial recognition to identify them.

In creating facial recognition templates, Facebook uses only data that people have voluntarily provided to Facebook: the photos and videos that people have voluntarily uploaded to Facebook (including public profile pictures) and the tags people have applied to those photos and videos. Facebook does not use facial recognition to identify someone to a stranger.

Question 80. Yes or no: does Facebook collect users' audio or visual information for any reason whatsoever, or otherwise activate, monitor, or capture data from a microphone or camera from a user's phone without the user's contemporaneous knowledge and express, contemporaneous consent? If so, please list each and every instance under which Facebook does so.

Answer. No, Facebook does not engage in these practices or capture data from a microphone or camera without consent. Of course, we do allow people to take videos on their devices and share those on our platform.

Question 81. Will Facebook commit to not using its platform to gather such audio or visual information surreptitiously?

Answer. See Response to Question 80.

Question 82. During the April 11, 2018 House Energy and Commerce Hearing, you stated, "there may be specific things about how you use Facebook, even if you're not logged in, that we keep track of, to make sure that people aren't abusing the systems." You further stated that "in general, we collect data on people who have not signed up for Facebook for security purposes."

(a) What categories of data does Facebook collect about registered users' activity on websites and mobile applications other than Facebook?

(b) What categories of data does Facebook collect about individuals who are not registered Facebook users and their activity on websites and mobile applications other than Facebook?

(c) To the extent Facebook collects such data, does Facebook sell or provide this data to third parties?

(d) To the extent Facebook collects such data, has Facebook gained consent from those individuals to collect and use their personal data?

(e) To the extent Facebook gathers such data, what opportunity does Facebook provide to individuals not using Facebook to know, correct, or delete any information Facebook has gathered and retained about them?

Answer. See Response to Question 74.

When the individual is a Facebook user, we are also able to use this information to personalize their experiences on Facebook, whether or not they are logged out, but we will not target ads to users relying on this information unless the user allows this in their privacy settings. We do not sell or share this information with third-parties.

Question 83. Most of your answers to the questions you received on April 10, 2018, and likely most of the answers to these questions for the record, will depend on information that Facebook alone possesses.

(a) Why is/are Facebook's content-suggesting algorithm(s) secret?

(b) Why are Facebook's editorial decisions secret?

Answer. See Response to Question 74.

When the individual is a Facebook user, we are also able to use this information to personalize their experiences on Facebook, whether or not they are logged out, but we will not target ads to users relying on this information unless the user allows this in their privacy settings. We do not sell or share this information with third-parties.

Question 84. Numerous Americans receive all or a significant portion of their news from Facebook, which, in turn, suggests that news to them based on an algorithm that determines appropriate content based on criteria known only to Facebook.

(a) To what extent will Facebook make public the criteria on which this algorithm relies?

(b) To what extent will Facebook make public any changes that it makes to this or similar algorithms?

Answer. Facebook is a distribution platform that reflects the conversations already taking place in society. We want Facebook to be a place where people can discover more news, information, and perspectives, and we are working to build products that help.

As to the questions regarding ranking and algorithmic changes, see Response to Question 47.

Question 85. Facebook conducts numerous social experiments on its users, examining everything from the effects of Facebook on voter turnout to the effects of Facebook on the mood of its users.

(a) Will Facebook commit to not experimenting on its users without express, informed consent in advance?

(b) Will Facebook commit to making the results of any such experiments known publicly?

(c) Will Facebook commit to not experimenting on human subjects at all?

Answer. Facebook does research in a variety of fields, from systems infrastructure to user experience to artificial intelligence to social science. We do this work to understand what we should build and how we should build it, with the goal of improving the products and services we make available each day. We're committed to doing research to make Facebook better, but we want to do it in the most responsible way.

In October 2014, we announced a new framework that covers both internal work and research that might be published:

- Guidelines: we've given researchers clearer guidelines. If proposed work is focused on studying particular groups or populations (such as people of a certain age) or if it relates to content that may be considered deeply personal (such as emotions) it will go through an enhanced review process before research can begin. The guidelines also require further review if the work involves a collaboration with someone in the academic community.
- Review: we've created a panel including our most senior subject-area researchers, along with people from our engineering, research, legal, privacy and policy teams, that will review projects falling within these guidelines. This is in addition to our existing privacy cross-functional review for products and research.
- Training: we've incorporated education on our research practices into Facebook's six-week training program, called bootcamp, that new engineers go through, as well as training for others doing research. We'll also include a section on research in the annual privacy and security training that is required of everyone at Facebook.

- Research website: our published academic research is now available at a single location (*https://research.facebook.com/*) and will be updated regularly.

We believe in research because it helps us build a better Facebook. Like most companies today, our products are built based on extensive research, experimentation and testing.

It's important to engage with the academic community and publish in peer-reviewed journals, to share technology inventions and because online services such as Facebook can help us understand more about how the world works. We want to do this research in a way that honors the trust users put in us by using Facebook every day. We will continue to learn and improve as we work toward this goal.

Question 86. What, if any, procedures does Facebook employ to verify the identities of individuals who purchase or employ data from Facebook?

Answer. Facebook does not sell people's information to anyone, and we never will. We also impose strict restrictions on how our partners can use and disclose the data we provide.

Our Data Policy makes clear the circumstances in which we work with third-party partners who help us provide and improve our Products or who use Facebook Business Tools to grow their businesses, which makes it possible to operate our companies and provide free services to people around the world.

Question 87. Research and reporting by NYU Professor of Marketing Scott Galloway suggests that, combined, Facebook and Google (parent company now known as Alphabet) are together worth approximately $1.3 trillion. He concludes that this figure exceeds the world's top five advertising agencies (WPP, Omnicom, Publicis, IPG, and Dentsu) with five major media companies (Disney, Time Warner, 21st Century Fox, CBS, and Viacom) and still need to add five major communications companies (AT&T, Verizon, Comcast, Charter, and Dish) approach 90 percent of Facebook and Google's combined worth.

(a) What business or product lines does Facebook consider itself to be in?

(i) On what basis does Facebook make that determination?

(ii) Who does Facebook consider its major competitors in each of these business or product lines?

(b) Of those business or product lines, what market share does Facebook believe that it has?

(c) What other entities provide *all* of the services that Facebook does in one place or platform, if any?

(d) What other entities provide *any* of the services that Facebook does?

(e) What is the relevant product market for Facebook (the platform)?

(f) What are the relevant product markets for each of Facebook's products?

(g) What is the relevant geographic market for Facebook (the platform)?

(h) What is the relevant geographic market for each of Facebook's products?

(i) Given these relevant geographic and product markets, what is Facebook's market share in each distinct market in which it operates?

(j) What procedures, tools, programs, or calculations does Facebook use to ascertain its market position relevant to its five largest competitors overall (if five exist)?

(k) What procedures, tools, programs, or calculations does Facebook use to ascertain its market position relevant to its five largest competitors in each product market (if five exist)?

Answer. In Silicon Valley and around the world, new social apps are emerging all the time. The average American uses eight different apps to communicate with their friends and stay in touch with people. There is a lot of choice, innovation, and activity in this space, with new competitors arising all the time. Facebook's top priority and core service is to build useful and engaging products that enable people to connect, discover and share through mobile devices and personal computers. Given its broad product offerings, Facebook faces numerous competitors, competing to attract, engage, and retain users, to attract and retain marketers, and to attract and retain developers who build compelling mobile and web applications. For instance, if a user wants to share a photo or video, they can choose between Facebook, DailyMotion, Snapchat, YouTube, Flickr, Twitter, Vimeo, Google Photos, and Pinterest, among many other services. Similarly, if a user is looking to message someone, just to name a few, there's Apple's iMessage, Telegram, Skype, Line, Viber, WeChat, Snapchat, and LinkedIn—as well as the traditional text messaging services their mobile phone carrier provides. Equally, companies also have more options than ever when it comes to advertising—from billboards, print and broadcast, to newer plat-

forms like Facebook, Spotify, Twitter, Google, YouTube, Amazon or Snapchat. Facebook represents a small part (in fact, just 6 percent) of this $650 billion global advertising ecosystem and much of that has been achieved by helping small businesses—many of whom could never have previously afforded newspaper or TV ads—to cost-effectively reach a wider audience.

Question 88. As you indicated in your testimony, Facebook's business model relies on advertising to individuals, typically through tailored advertisements. This means that Facebook has monetized access to the information that those individuals have published on Facebook.

(a) To Facebook's best approximation, what is the total value of all user information that Facebook has acquired or to which Facebook has access?

Answer. Facebook generates substantially all of its revenue from selling advertising placements to third parties. Our total revenue and the percentage of which comes from third-party ads is below. This information is from our SEC filings.

2017: 40,653,000,000 (98 percent from third party ads)
2016: 27,638,000,000 (97 percent from third party ads)
2015: 17,928,000,000 (95 percent from third party ads)
2014: 12,466,000,000 (92 percent from third party ads)
2013: 7,872,000,000 (89 percent from third party ads)
2012: 5,089,000,000 (84 percent from third party ads)
2011: 3,711,000,000 (85 percent from third party ads)
2010: 1,974,000,000 (95 percent from third party ads)
2009: 777,000,000
2008: 272,000,000

(b) How does Facebook categorize individual pieces of information for purposes of monetizing that information? (For example, Facebook acknowledges that if it is approached by a company selling ski equipment, it will target ads to individuals who have expressed an interest in skiing. We want to know in what ways Facebook organizes this information.)

Answer. As explained in our Data Policy, we collect three basic categories of data about people: (1) data about things people do and share (and who they connect with) on our services, (2) data about the devices people use to access our services, and (3) data we receive from partners, including the websites and apps that use our business tools. Our Data Policy provides more detail about each of the three categories. Any person can see each of the specific interests we maintain about them for advertising by visiting Ads Preferences, which lets people see what interests we use to choose ads for them—and to edit or delete these interests.

We use data from each of the categories described above to obtain these interests and to personalize every aspect of our services, which is the core value we offer and the thing that makes Facebook services unique from other online experiences. This includes selecting and ranking relevant content, including ads, posts, Page recommendations, to cite but a few examples.

For example, we use the data people provide about their age and gender to help advertisers show ads based on those demographics but also to customize the pronouns on our site and deliver relevant experiences to those users.

We use data about things people do on Facebook, such as the Pages they like, to associate "interests" with their accounts, so we can rank posts relating to those interests higher in NewsFeed, for example, or enable advertisers to reach audiences—*i.e.,* groups of people—that share those interests. For example, if a person has liked Pages about baseball, we might associate them with interests called "baseball" or "sports."

We use data from devices (such as location data) to help advertisers reach people in particular areas. For example, if people have shared their device locations with Facebook or checked into a specific restaurant, we can show them organic posts from friends who have been in that location or we can show them ads from an advertiser that wants to promote its services in their area or from the restaurant.

We also help advertisers reach people who have given the advertiser their contact information or who have used the advertiser's website or app. For example, advertisers can send us a hashed list of e-mail addresses of people they would like to reach on Facebook. If we have matching e-mail addresses, we can show those people ads from that advertiser (although we cannot see the e-mail addresses which are sent to us in hashed form, and these are deleted as soon as we complete the match).

Again, for people who are new to Facebook, we may have minimal data that we can use to personalize their experience, including their NewsFeed, their rec-

ommendations and the content (organic and sponsored) that they see. For people who have used our services for longer, we likely have more data, but the amount of data will depend on the nature of that use and how they have used our controls.

As noted above, in addition to general controls—such as Activity Log—we provide controls that specifically govern the use of data for ads. Through Ad Preferences, people see and control things like: (1) their "interests," which are keywords associated with a person based on activities such liking Pages and clicking ads; (2) their "behaviors" (which we also call "categories"), which generally reflect how, when and where they connect to Facebook; and (3) the advertisers that are currently showing them ads based on the person's contact information, based on the person's previous use of the advertiser's website or app, or based on a visit to the advertiser's store. People also can choose whether we use information about their activities on websites and apps off of Facebook to show them ads through Facebook, and whether we can use their Facebook advertising interests to show them ads off of Facebook. People's use of these controls will, of course, affect the data we use to show them ads.

(c) What types of advertisements does Facebook categorically prohibit?

Answer. Section 4 of our Advertising Policies list the types of ads that we categorically prohibit. These include ads that violate Community Standards, ads for illegal products and services, ads with adult content, ads that are misleading or false, ads that include profanity, and many more.

(d) What external controls restrict how Facebook monetizes, sells, rents, or otherwise commercializes an individual's information? Please include (separately) any laws that Facebook views as applicable, any injunctions presently binding Facebook, any regulations directing how Facebook may monetize information, and any publicly available, independent audits of how Facebook monetizes information.

Answer. Facebook complies with all applicable laws. In addition, we adhere to the commitments set forth in our Data Policy, which describes how we collect and use data.

(e) What internal controls restrict how Facebook monetizes, sells, rents, or otherwise commercializes an individual's information? Please include (separately) any internal policies, statements of ethics or principles, directives, guidelines, or prohibitions that Facebook routinely applies in determining whether to use an individual's personal information for commercial gain.

Answer. See Response to previous question.

Question 89. When an individual chooses to "lock down" or otherwise publicly conceal his Facebook profile, does Facebook:

(a) Continue to use that individual's private information for commercial gain? (This includes aggregating data as well as targeting advertisements at that individual.)

(b) Continue to retain that individual's private information for its own archives or records?

Answer. When people post on Facebook—whether in a status update or by adding information to their profiles—the ability to input the information is generally accompanied by an audience selector. This audience selector allows the person to choose who will see that piece of information on Facebook—whether they want to make the information public, share it with friends, or keep it for "Only Me." The tool remembers the audience a user shared with the last time they posted something and uses the same audience when the user shares again unless they change it. This tool appears in multiple places, such as privacy shortcuts and privacy settings. When a person makes a change to the audience selector tool in one place, the change updates the tool everywhere it appears. The audience selector also appears alongside things a user has already shared, so it's clear who can see each post. After a person shares a post, they have the option to change who it is shared with.

The audience with which someone chooses to share their information is independent of whether we use that information to personalize the ads and other content we show them. Specifically, our Data Policy explains that we may use any information that people share on Facebook "to deliver our Products, including to personalize features and content (including your News Feed, Instagram Feed, Instagram Stories and ads)." However, people can use our Ad Preferences tool to see the list of interests that we use to personalize their advertising. This means that, for example, a person who is interested in cars can continue to share that interest with their friends but tell us not to assign them an interest in ads for ad targeting purposes.

Likewise, the audience of a post does not determine whether a post is retained. Someone can choose to share a post with "Only Me" (meaning that they don't want anyone to see it but want to retain it in their Facebook account). They may also

choose to delete the information entirely. When people choose to delete something they have shared on Facebook, we remove it from the site. In most cases, this information is permanently deleted from our servers; however, some things can only be deleted when a user permanently deletes their account.

Question 90. What are Facebook's total advertising revenues for each of the calendar years 2001 to 2018?

Answer. Our total revenue and the percentage of which comes from third-party ads is below. This information is from our SEC filings.

2017: 40,653,000,000 (98 percent from third party ads)
2016: 27,638,000,000 (97 percent from third party ads)
2015: 17,928,000,000 (95 percent from third party ads)
2014: 12,466,000,000 (92 percent from third party ads)
2013: 7,872,000,000 (89 percent from third party ads)
2012: 5,089,000,000 (84 percent from third party ads)
2011: 3,711,000,000 (85 percent from third party ads)
2010: 1,974,000,000 (95 percent from third party ads)
2009: 777,000,000
2008: 272,000,000

(a) What are Facebook's online advertising revenues for each of the calendar years 2001 to 2018?

(b) What are Facebook's five largest competitors for online advertising in each year from 2001 to 2018?

(i) What were each of those competitors' advertising revenues through each of those years?

(ii) How many of Facebook's executive staff previously worked at each of those entities?

Answer. We expect that our competitors make their numbers available in their SEC filings. And, like many industries across the private sector, many people may work in multiple technology companies throughout the course of their careers.

Question 91. Regardless of place of incorporation, does Facebook consider itself an American company?

Answer. Yes, we're an American-based company where ninety percent of our community are outside the U.S.

Question 92. When Facebook makes policy decisions, are American citizens the company's top priority? If not, what is the company's top priority when it comes to policy decisions?

Answer. We are proud to be a U.S.-based company that serves billions of people around the world. While the majority of our employees are located here in the United States, more than 80 percent of the people who use Facebook are outside this country. We consider the needs of all of our users when making policy decisions. Of course, with headquarters in the U.S. and Ireland, we have particularly strong relationships with policy makers in those regions. We regularly engage with policy makers around the world, however, and work to take account of regional policy concerns as we build our products and policies for a global user base.

Question 93. Facebook, WhatsApp, and Instagram have all reportedly been blocked or partially blocked from the People's Republic of China (PRC) since 2009.

(a) Please describe the extent to which these services may be accessed from within the territory of the PRC, including Hong Kong and Macau, and describing in detail any geographical limits or limits on the available content.

Answer. Facebook, WhatsApp, and Instagram are available in Hong Kong and Macau. Facebook and Instagram are blocked in Mainland China. However, these can be accessed by people in Mainland China who employ VPNs. WhatsApp is typically available in Mainland China although we notice availability is often restricted around important events.

(b) On what basis does Facebook evaluate whether to honor a foreign government's request to block specific content?

Answer. When something on Facebook or Instagram is reported to us as violating local law, but doesn't go against our Community Standards, we may restrict the content's availability only in the country where it is alleged to be illegal after careful legal review. We receive reports from governments and courts, as well from non-government entities such as members of the Facebook community and NGOs.

(c) How does Facebook determine whether to honor a foreign government's request to block specific content or users?

Answer. See Response to previous question.

(d) Listed by country, what percentage of requests to block specific content (or users) from foreign governments does Facebook honor in whole or part?

Answer. This information is available here: *https://transparency.facebook.com/content-restrictions*.

(e) How does Facebook determine whether to honor the U.S. Government's request to block specific content or users?

Answer. Our Transparency Report contains data on restrictions we place on content that does not violate community standards but that is alleged to violate local law. We do not have any such reports for the United States.

(f) What percentage of requests to block specific content (or users) from the U.S. Government does Facebook honor in whole or part?

Answer. See Response to previous question.

Question 94. Yes or no: Has Facebook made any alterations, modifications, or changes to the encryption security of WhatsApp in response to or as a result of the PRC government or any of its agencies or in order to comply with PRC law?

Answer. No.

(a) If so, what changes has Facebook made to the encryption security?

(b) Does Facebook program in "back doors" or other mechanisms to decrypt or otherwise decode encrypted information at a government's request?

Answer. No.

(i) If so, under what circumstances does Facebook decrypt such data?

(ii) If so, on what platforms does Facebook have such protocols?

(c) Does Facebook make WhatsApp or Facebook information available to the PRC government on a searchable basis?

Answer. No.

Question 95. Since 2014, the PRC government has held a World Internet Conference. Charles Smith, the co-founder of the non-profit censorship monitoring website GreatFire, described foreign guests of the Conference as "complicit actors in the Chinese censorship regime [that] are lending legitimacy to Lu Wei, the Cyberspace Administration of China and their heavy-handed approach to Internet governance. They are, in effect, helping to put all Chinese who stand for their constitutional right to free speech behind bars."

(a) How many Facebook employees have attended the PRC's World Internet Conference?

(b) Have any Facebook employees ever participated on any panels or advisory committees that are held or have been established by the World Internet Conference?

Answer. There have been four World Internet Conferences. Several Facebook employees have attended one or more of these four conferences.

(i) If so, please list the employees and the panels or high-level advisory committees they have participated on.

Answer. One Facebook representative, Vaughan Smith, has participated in World Internet Conference panels and keynotes alongside representatives of other leading U.S. technology companies, for example Tim Cook and Sundar Pichai. No employees participated in advisory committees. Mr. Smith has provided keynotes on AI, innovation and how Facebook is building the knowledge economy.

(ii) Has Facebook assisted other countries in designing regimes to monitor or censor Facebook content? If so, which countries, and under what circumstances? Please describe each.

Answer. When something on Facebook or Instagram is reported to us as violating local law, but doesn't go against our Community Standards, we may restrict the content's availability only in the country where it is alleged to be illegal after careful legal review. We receive reports from governments and courts, as well from non-government entities such as members of the Facebook community and NGOs. This information is available here: *https://transparency.facebook.com/content-restrictions*.

Government criticism does not violate our community standards, and we do not evaluate or categorize accounts based on whether they engage in government criticism.

See also Response to Question 93(c).

(c) Has Facebook ever provided any financial support to the World Internet Conference? If yes, please provide and itemize all financial support that has been provided to the World Internet Conference.

Answer. Facebook has not paid to participate in the World Internet Conference. In 2016 we paid $10,000 to rent exhibit space at the event to showcase Oculus VR which is manufactured in China.

Question 96. Has Facebook ever temporarily shut down or limited access to Facebook, WhatsApp, or Instagram within a country or a specific geographic area, at the request of a foreign government or agency, including but not limited to, the PRC, the Islamic Republic of Iran, Syria, the Russian Federation, and Turkey?

(a) If so, please describe each instance Facebook has complied with a foreign government's request to censor content or users, the requesting government, the provided justification for the government request, and a description of the content requested to be removed.

(b) Please describe what if any policies Facebook has in place governing Facebook's responses to government censorship requests.

Answer. We do not block access to Facebook products and services in areas where they are otherwise generally available on the basis of specific government requests. We may independently limit access to certain functionality—such as peer-to-peer payments or facial recognition—in some jurisdictions based on legal and regulatory requirements.

In some instances, we may receive requests from governments or other parties to remove content that does not violate our Community Standards but is alleged to contravene local law. When we receive such requests, we conduct a careful review to confirm whether the report is legally valid and is consistent with international norms, as well as assess the impact of our response on the availability of other speech. When we comply with a request, we restrict the content only within the relevant jurisdiction. We publish details of content restrictions made pursuant to local law, as well as details of our process for handling these requests, in our Transparency Report (*https://transparency.facebook.com/content-restrictions*).

Response to Written Questions Submitted by Hon. Deb Fischer to Mark Zuckerberg

Question 1. Given ongoing user privacy concerns, American consumers are asking for a public dialogue about the *purposes* for which Facebook uses their personal data. However, a meaningful conversation cannot happen until users also understand the *sources* from which their data is gleaned, and the scope of the specific data—which characteristics, attributes, labels, or categories of data points—being collected and utilized. How many categories (*i.e.,* attributes, factors, labels, or data points) does Facebook collect about particular users?

Answer. As explained in our Data Policy, we collect three basic categories of data about people:

(1) data about things people do and share (and who they connect with) on our services;

(2) data about the devices people use to access our services; and

(3) data we receive from partners, including the websites and apps that use our business tools.

As far as the amount of data we collect about people, the answer depends on the person. People who have only recently signed up for Facebook have usually shared only a few things—such as name, contact information, age, and gender. Over time, as people use our products, we receive more data from them, and this data helps us provide more relevant content and services. That data will fall into the categories noted above, but the specific data we receive will, in large part, depend on how the person chooses to use Facebook. For example, some people use Facebook to share photos, so we receive and store photos for those people. Some people enjoy watching videos on Facebook; when they do, we receive information about the video they watched, and we can use that information to help show other videos in their News Feeds. Other people seldom or never watch videos, so we do not receive the same kind of information from them, and their News Feeds are likely to feature fewer videos.

The data we have about people also depends on how they have used our controls. For example, people who share photos can easily delete those photos. The same is true of any other kind of content that people post on our services. Through Facebook's Activity Log tool, people can also control the information about their en-

gagement—*i.e.,* their likes, shares and comments—with other people's posts. The use of these controls of course affects the data we have about people.

We recently announced improvements to our Download Your Information tool, as well as a new feature that makes it easier for people to see the information that's in their account on Facebook. These recently-expanded tools for accessing your information will allow people to see their data, delete it, and easily download and export it.

Question 2. How many categories, as the term is described above, are used to construct the digital profiles that Facebook utilizes to direct ads to particular users?

Answer. The specific number of categories that are used to decide what ads a person will see vary from person to person, depending on the interests and information that they have shared on Facebook, how frequently they interact with ads and other content on Facebook, and other factors. Any person can see each of the specific interests we maintain about them for advertising by visiting Ads Preferences, which lets people see what interests we use to choose ads for them—and to edit or delete these interests. We also provide more detailed information about how we use data to decide what ads to show to people in our "About Facebook Ads" page, at *https://www.facebook.com/ads/about.*

We use data about things people do on Facebook, such as the Pages they like, to associate "interests" with their accounts, and we enable advertisers to reach audiences—*i.e.,* groups of people—that share those interests. For example, if a person has liked Pages about baseball, we might associate them with interests called "baseball" or "sports."

We use data from devices (such as location data) to help advertisers reach people in particular areas. For example, if people have shared their device locations with Facebook or checked into a specific restaurant, we can show them ads from an advertiser that wants to promote its services in their area or from the restaurant.

We also help advertisers reach people who have given the advertiser their contact information or who have used the advertiser's website or app. For example, advertisers can send us a hashed list of e-mail addresses of people they would like to reach on Facebook. If we have matching e-mail addresses, we can show those people ads from that advertiser (although we cannot see the e-mail addresses which are sent to us in hashed form, and these are deleted as soon as we complete the match). The data we use to show ads to people depends on the data we have received from people. Again, for people who are new to Facebook, we may have minimal data that we can use. For people who have used our services for longer, we likely have more data, but the amount of data will depend on the nature of that use and how they have used our controls.

As noted above, in addition to general controls—such as Activity Log—we provide controls that specifically govern the use of data for ads. Through Ad Preferences, people see and control things like: (1) their "interests," which are keywords associated with a person based on activities such as liking Pages and clicking ads; (2) their "behaviors" (which we also call "categories"), which generally reflect how, when and where they connect to Facebook; and (3) the advertisers that are currently showing them ads based on the person's contact information, based on the person's previous use of the advertiser's website or app, or based on a visit to the advertiser's store. People also can choose whether we use information about their activities on websites and apps off of Facebook to show them ads through Facebook, and whether we can use their Facebook advertising interests to show them ads off of Facebook. People's use of these controls will, of course, affect the data we use to show them ads.

Question 3. If a user opts out of directed advertising, does Facebook halt collection of all such data?

Answer. We give people a number of controls over the data we use to show them ads. These controls apply to our use of data to show people ads; they do not apply to the collection of data, because the same core data sets are used to ensure the safety and security of our platform and to provide our core service to our users. As noted above, people can see and control the advertising "interests" and "behaviors" we have associated with their accounts to show them ads. They can choose not to see ads from a particular advertiser or not to see ads based on their use of third-party websites and apps. They also can choose not to see ads off Facebook that are based on the interests we derive from their activities on Facebook.

Question 4. If a user opts out of directed advertising, does Facebook delete all such data that was previously stored? Alternatively, does Facebook instead simply stop utilization of that data for directed advertising purposes?

Answer. Our advertising controls apply only to the use of data for targeting and selecting ads. Using these controls does not result in deletion of data, because the

same core data sets are used to ensure the safety and security of our platform and to provide our core service to our users. This is consistent with industry practice. For example, the Digital Advertising Alliance's Self-Regulatory Principles set the industry standard for the collection and use of data for online behavioral advertising and related practices. Those principles require companies to offer controls over the use of data for advertising purposes. Companies are not required to stop collecting data from opted-out users or to delete previously collected data. Please note, however, that when a person removes an "interest" or "behavior" in Ad Preferences, that interest or behavior is permanently removed from the person's ad profile; it will not be recreated even if the person subsequently engages in activities that otherwise would have resulted in the creation of the interest or behavior.

Question 5. When users download a copy of their Facebook data, as Facebook has recently enabled, is all ad targeting data included in that file?

Answer. Our Download Your Information or "DYI" tool is Facebook's data portability tool and was launched many years ago to let people access many types of information that we maintain about them, with a focus on those types that a person may wish to use on another online service. The data in DYI includes each of the demographic and interests-based attributes we use to show or target people ads. Although we do not store this data within DYI, people can also use Ad Preferences to see which advertisers are currently running ads based on their use of an advertiser's website or app. People also can choose not to see ads from those advertisers.

We are also launching Access Your Information, a screenshot of which was included in our April 27, 2018 letter to you. This is a secure way for people to access and manage their information. Users can go here to delete anything from their timeline or profile that they no longer want on Facebook. They can also see their ad interests, as well as information about ads they've clicked on and advertisers who have provided us with information about them that influence the ads they see. From here, they can go to their ad settings to manage how this data is used to show them ads.

Response to Written Questions Submitted by Hon. Jerry Moran to Mark Zuckerberg

Question 1. Cambridge Analytica had access to data on up to 87 million Facebook users because 270,000 individuals participated in a personality quiz that also exposed their friends' data. While I understand how the 270,000 individuals could have given their express consent, can you please walk me through how the many millions of friends could have given their "affirmative express consent" for their data to be shared with a third party as is required by the 2011 consent decree—when they were unaware that a friend of theirs was even participating in a personality quiz?

Answer. At the outset, we do not know what data Kogan may have shared with Cambridge Analytica. Our investigation into these matters is ongoing, and we are paused on investigating Cambridge Analytica directly (or conducting a forensic audit of its systems) due to the request of the UK Information Commissioner's Office, which is separately investigating Cambridge Analytica, a UK entity. The best information to date also suggests only U.S. user data was shared by Kogan with Cambridge Analytica.

As was the practice of other online or mobile app platforms, at that time, people on Facebook were able to take their data and data their friends had shared with them off of Facebook to apps they authorized to obtain a broader range of experiences than were available on Facebook. But people could not share data for friends whose privacy settings did not permit their data to be shared by their friends with apps—and no data was shared with Kogan's app in violation of friends' settings. The 2011 consent decree requires Facebook to get affirmative express consent for materially expanding the audience of a user's existing privacy settings. No privacy settings were expanded or exceeded on Platform, and the consent order therefore does not apply here.

Approximately 300,000 Facebook users worldwide installed Kogan's app. For the majority of these users, the app requested consent to access the following data fields associated with the user and with the friends of the user: Public profile data, including name and gender; Birthdate; "Current city" in the "About" section of the user's profile, if provided; and Facebook Pages liked.

For a small subset of users, it appears that the app also requested consent to access users' Facebook messages (fewer than 1,500 individuals, based on current information) and to posts that appeared in the user's News Feed or Timeline (approximately 100 individuals, based on current information)—but only for users who in-

stalled the app. For a small subset of users (fewer than 1,500 individuals, based on current information), it appears that the app also requested consent to access the hometowns that the users' friends had specified in the "About" section of their profiles. And for a handful of people (fewer than 10) who appear to be associated with Kogan/GSR, the app requested consent to e-mail address and photos.

Question 2. According to Facebook's March 21 press release, one of the six changes that Facebook initially offered to "crack down on platform abuse" was to reward outside parties who find vulnerabilities through its bug bounty program. My subcommittee has held hearings and met with interested stakeholders on these types of data security solutions along with other cyber vulnerability disclosure programs. One concern I have regarding the utility of this approach is that vulnerability disclosure programs are normally geared to identify unauthorized access to data, not point out data sharing arrangements that likely harm users but technically abide by the complex consent agreements Facebook pushes on their users. Could you please explain how Facebook's expansion of its bug bounty program will prevent future data sharing issues with its associated applications from occurring?

Answer. The Data Abuse Bounty will reward people with first-hand knowledge and proof of cases where a Facebook platform app collects and transfers people's data to another party to be sold, stolen or used for scams or political influence. We'll review all legitimate reports and respond as quickly as possible when we identify a credible threat to people's information. If we confirm data abuse, we will shut down the offending app and, if necessary, take legal action against the company selling or buying the data. We'll pay a bounty to the person who reported the issue, or allow them to donate their bounty to a charity, and we'll also alert those we believe to be affected. We also encourage our users to report to us content that they find concerning or that results in a bad experience, as well as other content that may violate our policies. We review these reports and take action on abuse, like removing content and disabling accounts.

Question 3. Facebook has confirmed alterations to its terms and conditions shifting more than 1.5 billion of its user from contracts with the international headquarters in Ireland to Facebook Inc. in the United States, thereby removing these users from the protections they would otherwise receive from the Europeans Union's General Data Protection Regulation (GDPR). With the recent scrutiny that Facebook has faced about its data collection, sharing, and security polices what is the justification for moving approximately 1.5 billion Facebook user away from the more stringent rules of the European Union's GDPR?

Answer. We will offer everyone who uses Facebook the same controls and settings, no matter where they live. However, the GDPR creates some specific requirements that do not apply in the rest of the world, for example the requirement to provide contact information for the EU Data Protection Officer or to specify legal bases for processing data. We are also looking to be more responsive to regional norms and legal frameworks going forward, and want to have the flexibility to work with local regulators, which is possible with this new model. At the same time, we are changing the provisions in our Facebook, Inc. terms in our user agreements outside the United States to allow people in other countries to file lawsuits against Facebook in their home country, rather than in courts in the U.S. This transition was part of a continued effort to be locally responsive in countries where people use our services.

Question 4. During your testimony, you noted that Facebook cooperates with law enforcement in two instances, where there is an "imminent threat of harm" or when law enforcement reaches out to the company with a "valid request for data." In December 2017, the Chicago Police Department announced that it had arrested fifty people who were utilizing Facebook private group features in order to communicate and facilitate illegal firearm and drug transactions. Several national news outlets reported that Facebook was not helpful in regards to this investigation and Chicago Police Superintendent Eddie Johnson was later quoted in response to media inquiries as saying "Quite frankly, they haven't been very friendly to law enforcement to prevent these things." What specific policies and procedures does Facebook currently have in place to aid law enforcement agencies in gaining access to relevant information that indicates a clear threat to public safety?

Answer. We recognize there are serious and evolving threats to public safety and that law enforcement has an important responsibility to keep people safe. Our legal and safety teams work hard to respond to legitimate law enforcement requests while fulfilling our responsibility to protect people's privacy and security. We have a global team that strives to respond within minutes to emergency requests from law enforcement. In the second half of 2017, for example, we provided information in response to nearly 78 percent of the 1,808 requests for emergency disclosures that we

received from U.S. law enforcement agencies. Facebook also reaches out to law enforcement whenever we see a credible threat of imminent harm. We use automated and manual review and also rely on users to help by reporting violating accounts or content. We are also working with law enforcement and others to improve our ability to find users at risk of harming themselves or others. We also disclose information in response to law enforcement requests in accordance with our terms of service and applicable law. In the second half of 2017, for example, we disclosed data in response to 85 percent of law enforcement requests from agencies in the U.S. Facebook regularly produces a report on government requests to help people understand the nature and extent of these requests and the policies and processes in place to handle them.

In addition, we cooperated with the Chicago Police Department's investigation that led to the December 2017 arrests. We reached out immediately after we learned of the comments referenced in your question, and they issued follow-up statements indicating that we reached out and were planning to provide training. We followed up by training over 100 Chicago-area law enforcement officers in a working group hosted by the FBI and U.S. Attorney's Office. We also met separately with the Chicago Police unit that conducted the investigation to make sure they understood Facebook's policies, how to submit requests to us, and how we could help them through additional training and support.

Question 5. What specifically qualifies as a "valid request for data," which is required to gain access to information?"

Answer. We disclose account records in accordance with our terms of service and applicable law, including the Federal Stored Communications Act. In the United States, a valid subpoena issued in connection with an official criminal investigation is required to compel the disclosure of basic subscriber records. A court order issued under 18 U.S.C. §2703(d) is required to compel the disclosure of certain records or other information pertaining to the account, not including contents of communications. A search warrant issued under the procedures described in the Federal Rules of Criminal Procedure or equivalent state warrant procedures upon a showing of probable cause is required to compel the disclosure of the stored contents of any account. Facebook may also voluntarily disclose information to law enforcement where we have a good faith reason to believe that the matter involves imminent risk of serious physical injury or death.

Question 6. How does Facebook determine what rises to an imminent threat of harm and does that determination change the threshold for deciding whether to respond to a law enforcement data request?

Answer. Facebook discloses account records in accordance with our terms of service and applicable law, including the Federal Stored Communications Act. The law permits Facebook to voluntarily disclose information to law enforcement where we have a good faith reason to believe that the matter involves imminent risk of serious physical injury or death. Our law enforcement response team receives and responds to emergency data requests around the clock and from around the globe based on our timely and careful review of information submitted by law enforcement and any other relevant facts. We also rely on experience and input from law enforcement, safety organizations, and industry to identify and respond to potential threats of harm.

Question 7. Facebook has made a big deal about users' ability to request and download the data that Facebook has compiled about the user. But that downloaded data does not include data such as the list of the websites Facebook users have visited that is collected by Facebook. Why is that the case, and when will Facebook make this information available to users? What other information about Facebook users is not available for download?

Answer. Our Download Your Information or "DYI" tool is Facebook's data portability tool and was launched many years ago to let people access and download many types of information that we maintain about them. The data in DYI and in our Ads Preferences tool contain each of the interest categories that are used to show people ads, along with information about the advertisers are currently running ads based on their use of an advertiser's website or app. People also can choose not to see ads from those advertisers. We recently announced expansions to Download Your Information, which, among other things, will make it easier for people to see their data, delete it, and easily download and export it. More information is available at *https://newsroom.fb.com/news/2018/04/new-privacy-protections.*

Responding to feedback that we should do more to provide information about websites and apps that send us information when people use them, we also announced plans to build Clear History. This new feature will enable users to see the websites and apps that send us information when they use them, delete this infor-

mation from their account, and turn off Facebook's ability to store it associated with their account going forward.

We have also introduced Access Your Information. This feature provides a new way for people to access and manage their information. Users can go here to delete anything from their timeline or profile that they no longer want on Facebook. They can also see their ad interests, as well as information about ads they've clicked on and advertisers who have provided us with information about them that influence the ads they see. From here, they can go to their ad settings to manage how this data is used to show them ads.

RESPONSE TO WRITTEN QUESTIONS SUBMITTED BY HON. DAN SULLIVAN TO MARK ZUCKERBERG

Question 1. In the hearing, the topics of anticompetitive consolidation and the enormous market capitalization of tech companies such as Facebook were frequently raised. Recent calculations value the four largest tech companies' capitalization at $2.8 trillion dollars, which is a staggering 24 percent of the S&P 500 Top 50, close to the value of every stock traded on the Nasdaq in 2001, and to give a different perspective, approximately the same amount as France's current GDP. At what point, from an antitrust perspective, is Facebook simply too big? Would you say that your size inhibits the "next Facebook"?

Answer. In Silicon Valley and around the world, new social apps are emerging all the time. The average American uses eight different apps to communicate with their friends and stay in touch with people. There is a lot of choice, innovation, and activity in this space, with new competitors arising all the time. Facebook's top priority and core service is to build useful and engaging products that enable people to connect, discover and share through mobile devices and personal computers. Given its broad product offerings, Facebook faces numerous competitors, competing to attract, engage, and retain users, to attract and retain marketers, and to attract and retain developers who build compelling mobile and web applications. For instance, if you want to share a photo or video, you can choose between Facebook, DailyMotion, Snapchat, YouTube, Flickr, Twitter, Vimeo, Google Photos and Pinterest among many other services. Similarly, if you are looking to message someone, just to name a few, there's Apple's iMessage, Telegram, Skype, Line, Viber, WeChat, Snapchat and LinkedIn—as well as the traditional text messaging services your mobile phone carrier provides. Equally, companies also have more options than ever when it comes to advertising—from billboards, print and broadcast, to newer platforms like Facebook, Spotify, Twitter, Google, YouTube, Amazon, or Snapchat. Facebook represents a small part (in fact, just 6 percent) of this $650 billion global advertising ecosystem and much of that has been achieved by helping small businesses—many of whom could never have previously afforded newspaper or TV ads—to cost-effectively reach a wider audience.

Question 2. Senator Peters asked if Facebook extracts audio from its users to enhance personal data profiles, to which you responded no—is that the case? There are countless anecdotes about this exact situation. Would you characterize these as coincidence or is targeted advertising just that effective?

Answer. To be crystal clear on this point: Facebook does not use users' phone's microphone or any other method to extract audio to inform ads or to determine what they see in their News Feed. Facebook show ads based on people's interests and other profile information—not what users are talking out loud about. Facebook only accesses users' microphone if the user has given our app permission and if they are actively using a specific feature that requires audio (like voice messaging features).

Question 3. As you are aware, children are increasingly active users of technology. Do you have concerns generally about children's increased use, in many cases that rises to the level of addiction, of electronics? And more specifically, since I'm very interested in the issue of individual privacy rights, what are your thoughts on the data footprint of children being collected?

Answer. We take the privacy, safety, and security of all those who use our platform very seriously and when it comes to minors (13 to 18 years old), we provide special protections and resources.

We also provide special protections for teens on Facebook and Messenger. We provide education before allowing teens to post publicly. We don't show search results based on specific profile data (high school, birthday/age, and hometown, or current city) of teens to unconnected adults when the adults search on Facebook. Unconnected adults can't message minors who are 13–17. We prohibit search engines off Facebook from indexing minors' profiles. And, we have age limits for adver-

tisements. For example, ads for dating sites, financial services and other products or services are gated to users under 18.

We provide special resources to help ensure that they enjoy a safe and secure experience. For example, we recently announced the launch of our Youth Portal, which is available in 60 languages at facebook.com/safety/youth. This portal is a central place for teens that includes:

- *Education:* Information on how to get the most out of products like Pages, Groups, Events, and Profile, while staying safe. Plus, information on the types of data Facebook collects and how we use it.
- *Peer Voices:* First person accounts from teens around the world about how they are using technology in new and creative ways.
- *Ways to control your experience:* Tips on things like security, reporting content, and deciding who can see what teens share.
- *Advice:* Guidelines for how to safely get the most out of the internet.

Instagram also will be providing information to teens to show them where they can learn about all of the tools on Instagram to manage their privacy and stay safe online, including how to use the new Access and Download tools to understand what they have shared online and learn how to delete things they no longer want to share. We are also making this information available in formats specifically designed for young users, including video tutorials for our privacy and safety tools, and teen-friendly FAQs about the Instagram Terms of Use, Data Policy, safety features, and Community Guidelines.

Instagram has also launched new content on Instagram Together, including videos and FAQs about privacy controls; information on how to use safety features, including comment controls, blocking accounts, reporting abuse, spam, or troubling messages; information on responsible social media use; and FAQs about safety on Instagram. We will be reaching out to users under 18 on Instagram to encourage them to learn more on Instagram Together.

Further, we have content restrictions and reporting features for everyone, including minors. We have Community Standards that prohibit hate speech, bullying, intimidation, and other kinds of harmful behavior. We encourage people to report posts and rely on our team of content reviewers around the world to review reported content. Our reviewers are trained to look for violations and enforce our policies consistently and as objectively as possible. When reviewed by our team, we hide certain graphic content from users under 18 (and include a warning for adults). We are also working to improve our ability to get our community help in real time, especially in instances where someone is expressing thoughts of suicide or self-harm, by expanding our use of proactive detection, working with safety experts and first-responders, and dedicating more reviewers from our Community Operations team.

In addition, with 9 out of 10 children under the age of 13 in the United States able to access a tablet or smartphone and 2 out of 3 with their own device, and parents seeking greater control over who connects with their children, the content they see and the time they spend online, we are committed to working with parents and families, as well as experts in child development, online safety and children's health and media, to ensure we are building better products for families.

That is why we're committed to both continued research and to building tools that promote meaningful interactions and help people manage their time on our platform.

Indeed, as we built Messenger Kids, we worked closely with leading child development experts, educators, and parents to inform our decisions. Our advisors include experts in the fields of child development, online safety, and children's media currently and formerly from organizations such as the Yale Center for Emotional Intelligence, Connect Safely, Center on Media and Child Health, Sesame Workshop and more. The app does not have ads or in app purchase and we recently added Sleep Mode which gives the parent the ability to set parameters on when the app can be used. Messenger Kids collects only a limited amount of information. Additionally, when a Messenger Kids user turns 13, which the minimum age to join Facebook, they don't automatically get a Facebook account.

We recently launched a Parents Portal and Youth Portal, which are both focused on fostering conversations around online safety and giving parents and young people access to the information and resources they need to make informed decisions about their use of online technologies.

Question 4. I'm very proud to be a cosponsor of the recently passed SESTA legislation, which as you know, takes serious steps to hold websites and other institutions accountable that knowingly facilitate sex trafficking activity by closing loopholes in what was outdated Federal communications law. As an active participant in the de-

liberations and negotiations throughout the process, I noticed that while Facebook ultimately supported the legislation, that was a stance that evolved significantly–can you explain Facebook's shifting views on this bill?

Answer. Facebook supports SESTA. We support the goal of the legislation of providing victims of sex trafficking with recourse in the courts against parties who directly support these illegal activities, but wanted to ensure that good actors were not penalized for their efforts to root out this type of harm online. We were very pleased to be able to work successfully with a bipartisan group of Senators on a bill that protects women and children from the harms of sex trafficking.

Facebook is committed to making our platform a safe place, especially for individuals who may be vulnerable. We have a long history of working successfully with governments to address a wide variety of threats to our platform, including child exploitation. When we learn of a situation involving physical abuse, child exploitation, or an imminent threat of harm to a person, we immediately report the situation to first responders or the National Center for Missing and Exploited Children (NCMEC).

Further, as part of official investigations, government officials sometimes request data about people who use Facebook. We have processes in place to handle these government requests, and we disclose account records in accordance with our terms of service and applicable law. We also have a global team that strives to respond within minutes to emergency requests from law enforcement.

Our relationship with NCMEC also extends to an effort that we launched in 2015 to send AMBER Alerts to the Facebook community to help find missing children. When police determine that a case qualifies for an AMBER Alert, the alert is issued by the NCMEC and distributed through the Facebook system with any available information, including a photograph of the missing child, a license plate number, and the names and descriptions of the child and suspected abductor. Law enforcement determines the range of the target area for each alert. We know the chances of finding a missing child increase when more people are on the lookout, especially in the critical first hours. Our goal is to help get these alerts out quickly to the people who are in the best position to help, and a number of missing children have been found through AMBER Alerts on Facebook.

Further, we work tirelessly to identify and report child exploitation images (CEI) to appropriate authorities. We identify CEI through a combination of automated and manual review. On the automated review side, we use image hashing to identify known CEI. On the manual review side, we provide in-depth training to content reviewers on how to identify possible CEI. Confirmed CEI is reported to the NCMEC, which then forwards this information to appropriate authorities. When we report content to the NCMEC, we preserve account information in accordance with applicable law, which can help further law enforcement investigations. We also reach out to law enforcement authorities in serious cases to ensure that our reports are received and acted upon.

Question 5. Were your terms of service for third party app developers violated by Cambridge Analytica? If not, have they ever been violated in the past and what were those situations and outcomes?

Answer. Cambridge Analytica signed certifications at our insistence declaring that they had deleted all copies of Facebook data and derivatives obtained from Kogan's app. In March 2018, we received reports that, contrary to the certification and confirmation we were given by SCL/Cambridge Analytica, not all data was deleted. We are moving aggressively to determine the accuracy of these claims. If true, this is an unacceptable violation of trust and a breach of the representations Cambridge Analytica made in the certifications.

Question 6. Can a user opt-out of Facebook collecting and compiling a user's web browsing history? If so, please provide the details regarding how a user opts out of this collection.

Answer. The Ad Preferences tool on Facebook shows people the advertisers whose ads the user might be seeing because they visited the advertisers' sites or apps. The person can remove any of these advertisers to stop seeing their ads.

In addition, the person can opt out of these types of ads entirely—so he or she never sees those ads on Facebook based on information we have received from other websites and apps.

We've also announced plans to build Clear History, a feature that will enable people to see the websites and apps that send us information when they use them, delete this information from their accounts, and turn off our ability to store it associated with their accounts going forward.

Apps and websites that use features such as the Like button or Facebook Analytics send us information to make their content and ads better. We also use this

information to make user experience on Facebook better. If a user clears his or her history or uses the new setting, we'll remove identifying information so a history of the websites and apps the user used won't be associated with the user's account. We'll still provide apps and websites with aggregated analytics—for example, we can build reports when we're sent this information so we can tell developers if their apps are more popular with men or women in a certain age group. We can do this without storing the information in a way that's associated with the user's account, and as always, we don't tell advertisers who users are.

It will take a few months to build Clear History. We'll work with privacy advocates, academics, policymakers, and regulators to get their input on our approach, including how we plan to remove identifying information and the rare cases where we need information for security purposes. We've already started a series of roundtables in cities around the world and heard specific demands for controls like these at a session we held at our headquarters. We're looking forward to doing more.

Question 7. Finally, since you've recently spent some time in Alaska, I'm sure your travels gave you a sense for our ardent individualism and general skepticism about the benefits of conceding privacy in the name of security. How can my constituents be assured of their security online? Or more generally, what would you say should be their new expectation of privacy online?

Answer. We believe that everyone has the right to expect strong protections for their information, and that we also need to do our part to help keep our community safe, in a way that's consistent with people's privacy expectations. We've recently announced several steps to give people more control over their privacy, including a new Privacy Shortcuts tool that we're rolling out now to give people information about how to control their information, including choosing who can see what they post and adding protections like two-factor authentication to their account. People can learn more about how to protect their privacy in our updated Data Policy and in our Privacy Basics feature (*https://www.facebook.com/about/basics*).

RESPONSE TO WRITTEN QUESTIONS SUBMITTED BY HON. BILL NELSON TO MARK ZUCKERBERG

Question 1. While the primary focus of the April 10 hearing was on Cambridge Analytica and Facebook's privacy and data security policies, concerns were heard about many other issues from Members on both sides of the aisle. Within this context, please detail specific steps that Facebook is taking to address: (1) "fake news", (2) foreign government interference in American elections, (3) illegal sex trafficking, and (4) copyright infringement of digital content.

Answer. *Fake News:* We are working hard to stop the spread of false news. We work with third party fact checking organizations to limit the spread of articles with rated false. To reduce the spread of false news, we remove fake accounts and disrupt economic incentives for traffickers of misinformation. We also use various signals, including feedback from our community, to identify potential false news. In countries where we have partnerships with independent third-party fact-checkers, stories rated as false by those fact-checkers are shown lower in News Feed. If Pages or domains repeatedly create or share misinformation, we significantly reduce their distribution and remove their advertising rights. We also want to empower people to decide for themselves what to read, trust, and share. We promote news literacy and work to inform people with more context. For example, if third-party fact-checkers write articles about a news story, we show them immediately below the story in the Related Articles unit. We also notify people and Page Admins if they try to share a story, or have shared one in the past, that's been determined to be false. In addition to our own efforts, we're learning from academics, scaling our partnerships with third-party fact-checkers and talking to other organizations about how we can work together.

Foreign Interference: In the run-up to the 2016 elections, we were focused on the kinds of cybersecurity attacks typically used by nation states, for example phishing and malware attacks. And we were too slow to spot this type of information operations interference. Since then, we've made important changes to prevent bad actors from using misinformation to undermine the democratic process. This will never be a solved problem because we're up against determined, creative and well-funded adversaries. But we are making steady progress. Here is a list of the 10 most important changes we have made:

- *Ads transparency.* Advertising should be transparent: users should be able to see all the ads an advertiser is currently running on Facebook, Instagram, and

Messenger. We are taking steps to help users assess the content they see on Facebook. For example, for ads with political content, we've created an archive that will hold ads with political content for seven years—including for information about ad impressions and spend, as well as demographic data such as age, gender, and location. People in Canada and Ireland can already see all the ads that a Page is running on Facebook—and we're launching this globally in June. Further, advertisers will now need to confirm their ID and location before being able to run any ads with political content in the U.S. All ads with political content will also clearly state who paid for them. We also want to empower people to decide for themselves what to read, trust, and share. We promote news literacy and work to inform people with more context. For example, if third-party fact-checkers write articles about a news immediately below the story in the Related Articles unit. We also notify people and Page Admins if they try to share a story, or have shared one in the past, that's been determined to be false.

- *Verification and labeling.* We are working hard to regain the trust of our community. Success would consist of minimizing or eliminating abuse of our platform and keeping our community safe. We have a number of specific goals that we will use to measure our progress in these efforts. First, we are increasing the number of people working on safety and security at Facebook, to 20,000. We have significantly expanded the number of people who work specifically on election integrity, including people who investigate this specific kind of abuse by foreign actors. Those specialists find and remove more of these actors. Second, we work to improve threat intelligence sharing across our industry, including, we hope, by having other companies join us in formalizing these efforts. This is a fight against sophisticated actors, and our entire industry needs to work together to respond quickly and effectively. Third, we are bringing greater transparency to election ads on Facebook by requiring more disclosure from people who want to run election ads about who is paying for the ads and by making it possible to see all of the ads that an advertiser is running, regardless of the targeting. We believe that these efforts will help to educate our community and to arm users, media, civil society, and the government with information that will make it easier to identify more sophisticated abuse to us and to law enforcement.
- *Updating targeting.* We want ads on Facebook to be safe and civil. We thoroughly review the targeting criteria advertisers can use to ensure they are consistent with our principles. As a result, we removed nearly one-third of the targeting segments used by the IRA. We continue to allow some criteria that people may find controversial. But we do see businesses marketing things like historical books, documentaries or television shows using them in legitimate ways.
- *Better technology.* We have gotten increasingly better at finding and disabling fake accounts. We're now at the point that we block millions of fake accounts each day at the point of creation before they do any harm. This is thanks to improvements in machine learning and artificial intelligence, which can proactively identify suspicious behavior at a scale that was not possible before—without needing to look at the content itself.
- *Action to tackle fake news.* (see above).
- *Significant investments in security.* We're doubling the number of people working on safety and security from 10,000 last year to over 20,000 this year. We expect these investments to impact our profitability. But the safety of people using Facebook needs to come before profit.
- *Industry collaboration.* In April, we joined 34 global tech and security companies in signing a TechAccord pact to help improve security for everyone.
- *Intelligence sharing with government.* In the 2017 German elections, we worked closely with the authorities there, including the Federal Office for Information Security (BSI). This gave them a dedicated reporting channel for security issues related to the Federal elections.
- *Tracking 40+ elections.* In recent months, we've started to deploy new tools and teams to proactively identify threats in the run-up to specific elections. We first tested this effort during the Alabama Senate election, and plan to continue these efforts for elections around the globe, including the U.S. midterms. Last year we used public service announcements to help inform people about fake news in 21 separate countries, including in advance of French, Kenyan and German elections.
- *Action against the Russia-based IRA.* In April, we removed 70 Facebook and 65 Instagram accounts—as well as 138 Facebook Pages—controlled by the IRA primarily targeted either at people living in Russia or Russian-speakers around

the world including from neighboring countries like Azerbaijan, Uzbekistan, and Ukraine. The IRA has repeatedly used complex networks of inauthentic accounts to deceive and manipulate people in the U.S., Europe, and Russia—and we don't want them on Facebook anywhere in the world. We are taking steps to enhance trust in the authenticity of activity on our platform, including increasing ads transparency, implementing a more robust ads review process, imposing tighter content restrictions, and exploring how to add additional authenticity safeguards. We also have improved information sharing about these issues among our industry partners.

Copyright: Facebook takes intellectual property rights seriously and believes they are important to promoting expression, creativity, and innovation in our community. Facebook's Terms of Service do not allow people to post content that violates someone else's intellectual property rights, including copyright and trademark. We publish information about the intellectual property reports we receive in our bi-annual Transparency Report, which can be accessed at *https://transparency.facebook.com/*

Sex trafficking: Facebook is committed to making our platform a safe place, especially for individuals who may be vulnerable. We have a long history of working successfully with governments to address a wide variety of threats to our platform, including child exploitation.

When we learn of a situation involving physical abuse, child exploitation, or an imminent threat of harm to a person, we immediately report the situation to first responders or the National Center for Missing and Exploited Children (NCMEC). Further, as part of official investigations, government officials sometimes request data about people who use Facebook. We have processes in place to handle these government requests, and we disclose account records in accordance with our terms of service and applicable law. We also have a global team that strives to respond within minutes to emergency requests from law enforcement.

Our relationship with NCMEC also extends to an effort that we launched in 2015 to send AMBER Alerts to the Facebook community to help find missing children. When police determine that a case qualifies for an AMBER Alert, the alert is issued by the NCMEC and distributed through the Facebook system with any available information, including a photograph of the missing child, a license plate number, and the names and descriptions of the child and suspected abductor. Law enforcement determines the range of the target area for each alert. We know the chances of finding a missing child increase when more people are on the lookout, especially in the critical first hours. Our goal is to help get these alerts out quickly to the people who are in the best position to help, and a number of missing children have been found through AMBER Alerts on Facebook.

Further, we work tirelessly to identify and report child exploitation images (CEI) to appropriate authorities. We identify CEI through a combination of automated and manual review. On the automated review side, we use image hashing to identify known CEI. On the manual review side, we provide in-depth training to content reviewers on how to identify possible CEI. Confirmed CEI is reported to the NCMEC, which then forwards this information to appropriate authorities. When we report content to the NCMEC, we preserve account information in accordance with applicable law, which can help further law enforcement investigations. We also reach out to law enforcement authorities in serious cases to ensure that our reports are received and acted upon.

Question 2. Some commentators worry that the Internet is dominated by a few large platforms with little competition or accountability. Facebook is obviously considered to be one of those key, dominant platforms.

- Please comment on how American laws should hold large Internet platforms accountable when things go wrong?
- What is Facebook's legal and ethical responsibility as an Internet platform with billions of global users?

Answer. Our mission is to give people the power to build community and bring the world closer together—a mission that is inherently global and enhanced by a global scope. As the Internet becomes more important in people's lives, the real question is about the right set of regulations that should apply to all Internet services, regardless of size. Across the board, we have a responsibility to not just build tools, but to make sure that they're used in ways that are positive for our users. It will take some time to work through all the changes we need to make across the company, but Facebook is committed to getting this right.

Question 3. If large Internet platforms compromise consumer privacy and/or facilitate the theft of original content, what should be the Federal Government's response? What should be the obligations of the platforms?

Answer. We take intellectual property rights seriously at Facebook and work closely with the motion picture industries and other rights holders worldwide to help them protect their copyrights and other IP. Our measures target potential piracy across our products, including Facebook Live, and continue to be enhanced and expanded. These include a global notice-and-takedown program, a comprehensive repeat infringer policy, integration with the content recognition service Audible Magic, and our proprietary video-and audio-matching technology called Rights Manager. More information about these measures can be found in our Intellectual Property Help Center, Transparency Report, and Rights Manager website.

Question 4. In general, as reflected in the General Data Protection Regulation (GDPR), the European Union (EU) is considered to require stronger data and privacy protections than the United States. According to press reports, Facebook will be moving 1.5 billion users outside of the scope of the EU's GDPR. Please explicitly lay out how Facebook's compliance with the GDPR will affect all Facebook users, including American users. That is, to what extent will the GDPR's requirements and protections extend to Americans and users outside Europe?

Answer. The press reports referred to in this question pertain to the legal entity with which Facebook users contract when they use the service, which changed in some jurisdictions as a part of the most recent updates to our Terms of Service and Data Policy. This change did not impact people who live in the United States, who contract with Facebook, Inc. under both our new and old policies.

The substantive protections in our user agreements offered by Facebook Ireland and Facebook, Inc. are the same. However, there are certain aspects of our Facebook Ireland Data Policy that are specific to legal requirements in the GDPR—such as the requirement that we provide contact information for our EU Data Protection Officer (DPO) or that we identify the "legal bases" we use for processing data under the GDPR. Likewise, our Facebook Ireland terms and Data Policy address the lawful basis for transferring data outside the EU, based on legal instruments that are applicable only to the EU.

In any case, the controls and settings that Facebook is enabling as part of GDPR are available to people around the world, including settings for controlling our use of face recognition on Facebook and for controlling our ability to use data we collect off Facebook Company Products to target ads. We recently began providing direct notice of these controls and our updated terms to people around the world (including in the U.S.), allowing people to choose whether or not to enable or disable these settings or to consent to our updated terms. We provide the same tools for access, rectification, erasure, data portability and others to people in the U.S. and rest of world that we provide in Europe, and many of those tools (like our Download Your Information tool, ad preferences tool, and Activity Log) have been available globally for many years.

Response to Written Questions Submitted by Hon. Maria Cantwell to Mark Zuckerberg

I understand that last week you announced your support for legislation that would regulate political ads on Internet platforms. By your own report, Facebook has removed 70 Facebook accounts, 138 Facebook Pages, and 65 Instagram accounts run by the Russian government-connected troll farm and election interference group known as the Internet Research Agency.

I want to explore the distinction between paid political ads and the troll and bot activity deployed by Russia that was designed to meddle with and influence U.S. elections.

Question 1. What tools do we have to address this going forward? If we pass the Honest Ads Act, won't we still have a problem with bots and trolls that aren't running traditional paid "political ads"?

Answer. We have always believed that Facebook is a place for authentic dialogue and that the best way to ensure authenticity is to require people to use the names they are known by. Fake accounts undermine this objective and are closely related to the creation and spread of inauthentic communication such as spam and disinformation. We also prohibit the use of automated means to access our platform. We rely on both automated and manual review in our efforts to effectively detect and deactivate fake accounts, including bots, and we are now taking steps to strengthen both. For example, we continually update our technical systems to identify, checkpoint, and remove inauthentic accounts. We block millions of attempts to register fake accounts every day. These systems examine thousands of detailed account attributes and prioritize signals that are more difficult for bad actors to disguise.

Question 2. Do we need a new definition of paid advertising or political expenditures that reaches bots and troll activity that are backed by foreign national interests?

Answer. We're committed to addressing this, and we have a number of efforts underway. Facebook has generally dealt with bots and troll activity via its Authenticity policy. Already, we build and update technical systems every day to better identify and remove inauthentic accounts, which also helps reduce the distribution of material that can be spread by accounts that violate our policies. Each day, we block millions of fake accounts at registration. Our systems examine thousands of account attributes and focus on detecting behaviors that are very difficult for bad actors to fake, including their connections to others on our platform. By constantly improving our techniques, we also aim to reduce the incentives for bad actors who rely on distribution to make their efforts worthwhile.

For example, the Internet Research Agency, based in St. Petersburg, is a "troll farm" and generally thought to be aligned with the Russian government. Facebook has determined that Internet Research Agency users violated Facebook's authenticity policy and has been working to remove them from the platform. This has resulted in the removal of numerous Facebook and Instagram accounts, as well as the content connected with those accounts. Facebook has found that many trolls are motivated by financial incentives and is taking steps to disrupt those incentives to discourage the behavior. While working to limit the impact of bots and trolls, Facebook is striving to strike the right balance between enabling free expression and ensuring that its platform is safe. Facebook's policies are aimed at encouraging expression and respectful dialogue.

Question 3. Would you commit to working on troll problem in a way that does not compromise free speech?

Answer. Yes, see Response to Question 2.

Question 4. In your testimony you talked about your use of artificial intelligence to combat hate speech, bots, and trolls. What do you feel is the correct regulatory or other approach Congress should take to address artificial intelligence or other emerging technologies?

Answer. Artificial Intelligence (AI) is a very promising technology that has many applications. Fairness, transparency and accountability should guide its development. Presently, AI systems make decisions in ways that people don't really understand. Thus, society needs to invest further in developing AI systems which are more transparent. Facebook has AI teams working on developing the philosophical, as well as technical, foundations for this work. We discussed our AI ethics work during the keynote of our recent developer's conference (at minute 47): *https://www.facebook.com/FacebookforDevelopers/videos/10155609688618553/*.

Question 5. How does Facebook plan to address the leveraging of its social engineering tools developed to optimize advertising revenue by state sponsored actors and geopolitical forces that seek to influence democratic elections and political outcomes?

Answer. In the run-up to the 2016 elections, we were focused on the kinds of cybersecurity attacks typically used by nation states, for example phishing and malware attacks. And we were too slow to spot this type of information operations interference. Since then, we've made important changes to prevent bad actors from using misinformation to undermine the democratic process.

This will never be a solved problem because we're up against determined, creative and well-funded adversaries. But we are making steady progress. Here is a list of the 10 most important changes we have made:

1. *Ads transparency.* Advertising should be transparent: users should be able to see all the ads an advertiser is currently running on Facebook, Instagram and Messenger. And for ads with political content, we've created an archive that will hold ads with political content for seven years—including information about ad impressions and spend, as well as demographic data such as age, gender and location. People in Canada and Ireland can already see all the ads that a Page is running on Facebook—and we're launching this globally in June.
2. *Verification and labeling.* Every advertiser will now need confirm their ID and location before being able to run any ads with political content in the U.S. All ads with political content will also clearly state who paid for them.
3. *Updating targeting.* We want ads on Facebook to be safe and civil. We thoroughly review the targeting criteria advertisers can use to ensure they are consistent with our principles. As a result, we removed nearly one-third of the targeting segments used by the IRA. We continue to allow some criteria that

people may find controversial. But we do see businesses marketing things like historical books, documentaries or television shows using them in legitimate ways.

4. *Better technology.* Over the past year, we've gotten increasingly better at finding and disabling fake accounts. We now block millions of fake accounts each day as people try to create them—and before they've done any harm. This is thanks to improvements in machine learning and artificial intelligence, which can proactively identify suspicious behavior at a scale that was not possible before—without needing to look at the content itself.
5. *Action to tackle fake news.* We are working hard to stop the spread of false news. We work with third party fact checking organizations to limit the spread of articles with rated false. To reduce the spread of false news, we remove fake accounts and disrupt economic incentives for traffickers of misinformation. We also use various signals, including feedback from our community, to identify potential false news. In countries where we have partnerships with independent third-party fact-checkers, stories rated as false by those fact-checkers are shown lower in News Feed. If Pages or domains repeatedly create or share misinformation, we significantly reduce their distribution and remove their advertising rights. We also want to empower people to decide for themselves what to read, trust, and share. We promote news literacy and work to inform people with more context. For example, if third-party fact-checkers write articles about a news story, we show them immediately below the story in the Related Articles unit. We also notify people and Page Admins if they try to share a story, or have shared one in the past, that's been determined to be false. In addition to our own efforts, we're learning from academics, scaling our partnerships with third-party fact-checkers and talking to other organizations about how we can work together.

   A key focus is working to disrupt the economics of fake news. For example, preventing the creation of fake accounts that spread it, banning sites that engage in this behavior from using our ad products, and demoting articles found to be false by fact checkers in News Feed—causing it to lose 80 percent of its traffic. We now work with independent fact checkers in the U.S., France, Germany, Ireland, the Netherlands, Italy, Mexico, Colombia, India, Indonesia and the Philippines with plans to scale to more countries in the coming months.
6. *Significant investments in security.* We're doubling the number of people working on safety and security from 10,000 last year to over 20,000 this year. We expect these investments to impact our profitability. But the safety of people using Facebook needs to come before profit.
7. *Industry collaboration.* Recently, we joined 34 global tech and security companies in signing a TechAccord pact to help improve security for everyone.
8. *Information sharing and reporting channels.* In the 2017 German elections, we worked closely with the authorities there, including the Federal Office for Information Security (BSI). This gave them a dedicated reporting channel for security issues related to the Federal elections.
9. *Tracking 40+ elections.* In recent months, we've started to deploy new tools and teams to proactively identify threats in the run-up to specific elections. We first tested this effort during the Alabama Senate election, and plan to continue these efforts for elections around the globe, including the U.S. midterms. Last year we used public service announcements to help inform people about fake news in 21 separate countries, including in advance of French, Kenyan and German elections.
10. *Action against the Russia-based IRA.* In April, we removed 70 Facebook and 65 Instagram accounts—as well as 138 Facebook Pages—controlled by the IRA primarily targeted either at people living in Russia or Russian-speakers around the world including from neighboring countries like Azerbaijan, Uzbekistan and Ukraine. The IRA has repeatedly used complex networks of inauthentic accounts to deceive and manipulate people in the U.S., Europe and Russia—and we don't want them on Facebook anywhere in the world.

Question 6. How should Congress address the leveraging of social engineering tools developed to optimize advertising revenue on technology platforms, by state sponsored actors and geopolitical forces that seek to influence democratic elections and political outcomes?

Answer. From its earliest days, Facebook has always been focused on security. These efforts are continuous and involve regular contact with law enforcement authorities in the U.S. and around the world. Elections are particularly sensitive

events for Facebook's security operations, and as the role of Facebook's service plays in promoting political dialogue and debate has grown, so has the attention of its security team. To address these concerns, Facebook is taking steps to enhance trust in the authenticity of activity on its platform, including increasing ads transparency, implementing a more robust ads review process, imposing tighter content restrictions, and exploring how to add additional authenticity safeguards. We welcome a dialog with government about how to address these societal issues.

Question 7. During the 2016 campaign, Cambridge Analytica worked with the Trump campaign to refine tactics. Were Facebook employees involved in that?

Answer. During the 2016 election cycle, Facebook worked with campaigns to optimize their use of the platform, including helping them understand various ad formats and providing other best practices guidance on use of the platform.

RESPONSE TO WRITTEN QUESTION SUBMITTED BY HON. AMY KLOBUCHAR TO MARK ZUCKERBERG

Question. Do you support a rule that would require you to notify your users of a breach within 72 hours?

Answer. Facebook is generally open to the idea of breach notification requirements, particularly legislation that would centralize reporting and ensure a consistent approach across the United States. For example, in Europe, the GDPR requires notification to a lead supervisory authority, rather than individual member states, in cases of a data breach. In the United States, however, there is no centralized notification scheme, and instead, reporting obligations vary widely across all 50 states. This complexity makes it harder to respond appropriately and swiftly to protect people in the event of a data breach. We believe this is an important issue and an area that is ripe for thoughtful regulation.

RESPONSE TO WRITTEN QUESTIONS SUBMITTED BY HON. RICHARD BLUMENTHAL TO MARK ZUCKERBERG

Question 1. Facebook's Download Your Information Tool: During the hearing, I asked not only whether Facebook users should be able to access their information, but specifically whether it would provide its users "all of the information that you collect as a result of purchases from data brokers, as well as tracking them?" You affirmatively stated that Facebook has a "Download Your Information (DYI) tool that allows people to see and to take out all of the information that they have put into Facebook or that Facebook knows about them."

However, in a March 7, 2018 correspondence provided to the U.K. Parliament regarding Paul-Olivier Dehaye's legal request for personal data, Facebook's Privacy Operations Team acknowledged that the DYI tool does not provide records stored in its 'Hive' database. This answer appears to confirm that the Facebook 'Pixel' web tracking system and other records are stored and combined with profile information, but not provided to users. Since then, *WIRED* magazine and academic researchers have noted the omission from the DYI tool of other pieces of data that Facebook is known to collect.

What specific pieces of data does Facebook collect that are not provided through the DYI tool? Please provide exact labels and descriptions of the types of data and its source, rather than broad categories or intent, including but not limited to web tracking data, location history, ad interactions and advertiser targeting data, third party applications, and derived inferences.

Answer. Our Download Your Information or "DYI" tool is Facebook's data portability tool and was launched many years ago to let people access and download many types of information that we maintain about them. The data in DYI and in our Ads Preferences tool contain each of the interest categories that are used to show people ads, along with information about the advertisers that are currently running ads based on their use of an advertiser's website or app. People also can choose not to see ads from those advertisers. We recently announced expansions to Download Your Information, which, among other things, will make it easier for people to see their data, delete it, and easily download and export it. More information is available at *https://newsroom.fb.com/news/2018/04/new-privacy-protections/*.

Responding to feedback that we should do more to provide information about websites and apps that send us information when people use them, we also announced plans to build Clear History. This new feature will enable users to see the websites and apps that send us information when they use them, delete this infor-

mation from their account, and turn off Facebook's ability to store it associated with their account going forward.

We have also introduced Access Your Information. This feature provides a new way for people to access and manage their information. Users can go here to delete anything from their timeline or profile that they no longer want on Facebook. They can also see their ad interests, as well as information about ads they've clicked on and advertisers who have provided us with information about them that influence the ads they see. From here, they can go to their ad settings to manage how this data is used to show them ads.

Question 2. Facebook's Web Tracking: While users can more readily understand the types of data that Facebook collects directly from them, Facebook's data collection practices regarding non-users and from other sources are opaque. For example, Facebook collects data from its social plugins, Pixel, and other similar properties ("web tracking data") that provide a deep understanding about an individual's web browsing habits.

Would an employee with appropriate technical permissions to the Hive database be able to generate a list of websites viewed by a Facebook user, where such websites contained a Facebook tracking property?

Answer. We have strict policy controls and technical restrictions so employees only access the data they need to do their jobs—for example to fix bugs, manage customer support issues or respond to valid legal requests. Employees who abuse these controls will be fired. Further information is available in our Cookies Policy, available at *http://facebook.com/ads/about.*

Question 3. Is web tracking data used for inferring an individual's interests or other characteristics? Are those inferences used in advertising?

Answer. Yes, but only for Facebook users. We do not use web browsing data to show ads to non-users or otherwise store profiles about non-users. Our goal is to show people content (including advertising) that is relevant to their interests. We use information people have provided on Facebook—such as things they've liked or posts they've engaged with—to help determine what people will be interested in. Like most online advertising companies, we also inform our judgments about what ads to show based on apps and websites that people use off of Facebook. People can turn off our use of web browser data and other data from third-party partners to show them ads through a control in Ads Preferences. They can also customize their advertising experience by removing interests that they do not want to inform the Facebook ads they see. In addition, a person's browser or device may offer settings that allow users to choose whether browser cookies are set and to delete them.

Question 4. Does Facebook provide users and non-users with the ability to disable the collection (not merely the use) of web tracking? Does Facebook allow users to delete this data without requiring the deletion of their accounts?

Answer. When people visit apps or websites that feature our technologies—like the Facebook Like or Comment button—our servers automatically log (i) standard browser or app records of the fact that a particular device or user visited the website or app (this connection to Facebook's servers occurs automatically when a person visits a website or app that contains our technologies, such as a Like button, and is an inherent function of Internet design); and (ii) any additional information the publisher of the app or website chooses to share with Facebook about the person's activities on that site (such as the fact that a purchase was made on the site). This is a standard feature of the Internet, and most websites and apps share this same information with multiple different third-parties whenever people visit their website or app. For example, the Senate Commerce Committee's website shares information with Google and its affiliate DoubleClick and with the analytics company Webtrends. This means that, when a person visits the Committee's website, it sends browser information about their visit to each one of those third parties. More information about how this works is available at *https://newsroom.fb.com/news/2018/04/data-off-facebook/*.

When the person visiting a website featuring Facebook's tools is not a registered Facebook user, Facebook does not have information identifying that individual, and it does not create profiles for this individual.

We use the browser and app logs that apps and websites send to us—described above—in the following ways for non-Facebook users. First, these logs are critical to protecting the security of Facebook and to detecting or preventing fake account access. For example, if a browser has visited hundreds of sites in the last five minutes, that's a sign the device might be a bot, which would be an important signal of a potentially inauthentic account if that browser then attempted to register for an account. Second, we aggregate those logs to provide summaries and insights to websites and apps about how many people visit or use their product or use specific

features like our Like button—but without providing any information about a specific person.

We do not create profiles for non-Facebook users, nor do we use browser and app logs for non-Facebook users to show targeted ads from our advertisers to them or otherwise seek to personalize the content they see. However, we may take the opportunity to show a general ad that is unrelated to the attributes of the person or an ad encouraging the non-user to sign up for Facebook.

When the individual is a Facebook user, we are also able to use this information to personalize their experiences on Facebook, whether or not they are logged out, but we will not target ads to users relying on this information unless the user allows this in their privacy settings. We do not sell or share this information with third-parties.

We recently announced plans to build on this by introducing Clear History, a new feature that will enable users to see the websites and apps that send us information when they use them, delete this information from their accounts, and turn off our ability to store it associated with their accounts going forward.

Question 5. One academic study from 2015 raised concerns about the privacy risks of web tracking data collected from health-related web pages, including an example of Facebook collecting information from the inclusion of a Facebook Like button on the CDC's page about HIV. Does Facebook impose any limitation on itself regarding the collection and use (including references) of web tracking data collected from health-related pages or any other themes of websites?

Answer. Websites and apps choose whether they use Facebook services to make their content and ads more engaging and relevant and whether they share browser data or other information with Facebook or other companies when people visit their sites. These services include:

- Social plugins, such as our Like and Share buttons, which make other sites more social and help people share content on Facebook;
- Facebook Login, which lets people use their Facebook account to log into another website or app;
- Facebook Analytics, which helps websites and apps better understand how people use their services; and
- Facebook ads and measurement tools, which enable websites and apps to show ads from Facebook advertisers, to run their own ads on Facebook or elsewhere, and to understand the effectiveness of their ads.

Many companies offer these types of services and, like Facebook, they also get information from the apps and sites that use them. Twitter, Pinterest, and LinkedIn all have similar Like and Share buttons to help people share things on their services. Google has a popular analytics service. And Amazon, Google, and Twitter all offer login features. These companies—and many others—also offer advertising services. In fact, most websites and apps send the same information to multiple companies each time users visit them.

For example, when a user visits a website, their browser (for example Chrome, Safari or Firefox) sends a request to the site's server. The browser shares a user's IP address, so the website knows where on the Internet to send the site content. The website also gets information about the browser and operating system (for example Android or Windows) they're using because not all browsers and devices support the same features. It also gets cookies, which are identifiers that websites use to know if a user has visited before.

A website typically sends two things back to a user's browser: first, content from that site; and second, instructions for the browser to send the user's request to the other companies providing content or services on the site. So, when a website uses one of our services, our users' browsers send the same kinds of information to Facebook as the website receives. We also get information about which website or app our users are using, which is necessary to know when to provide our tools.

Our policies include a range of restrictions on the use of these tools for health-related advertising. For example, we do not allow ads that discriminate based on disability, medical or genetic condition. Ads also may not contain content that directly or indirectly asserts or implies a person's disability, medical condition (including physical or mental health), or certain other traits. And ads generally may not request health information, including physical health, mental health, medical treatments, medical conditions, or disabilities. And we prohibit anyone from using our pixel to send us data that includes health, financial information, or other categories of sensitive information.

In addition, we also enable ad targeting options—called "interests" and "behaviors"—that are based on people's activities on Facebook, and when, where, and how

they connect to the Internet (such as the kind of device they use and their mobile carrier). These options do not reflect people's personal characteristics, but we still take precautions to limit the potential for advertisers to misuse them. For example, we do not create interest or behavior segments that suggest the people in the segment are members of sensitive groups such as people who have certain medical conditions.

Question 6. What changes, if any, is Facebook making to limit the amount of data that *Facebook itself* collects about users and non-users?

Answer. As explained in our Data Policy, we collect three basic categories of data about people: (1) data about things people do and share (and who they connect with) on our services, (2) data about the devices people use to access our services, and (3) data we receive from partners, including the websites and apps that use our business tools. Our Data Policy provides more detail about each of the three categories.

We use this information for a variety of purposes, including to provide, personalize, and improve our products, provide measurement, analytics, and other business services, promote safety and security, to communicate with people who use our services, and to research and innovate to promote the social good. We provide more information in our Data Policy about these uses as well.

Our policies limit our retention of the data that we receive in several ways. Specifically, we store data until it is no longer necessary to provide our services and Facebook products, or until a person's account is deleted—whichever comes first. This is a case-by-case determination that depends on things like the nature of the data, why it is collected and processed, and relevant legal or operational retention needs. For example, when a user searches for something on Facebook, they can access and delete that query from within their search history at any time, but the log of that search is deleted after 6 months. If they submit a copy of their government-issued ID for account verification purposes, we delete that copy 30 days after submission. If a user posts something on their Facebook profile, then that information would be retained until they delete it or until they delete their account.

We also have other policies that are designed to limit our retention of other types of information about people. For example, if a user visits a site with the "Like" button or another social plugin, we receive cookie information that we use to help show them a personalized experience on that site as well as Facebook, to help maintain and improve our service, and to protect both the user and Facebook from malicious activity. We delete or anonymize it within 90 days.

In general, when a user deletes their account, we delete things they have posted, such as their photos and status updates, and they won't be able to recover that information later. (Information that others have shared about them isn't part of their account and won't be deleted.)

There are some limited exceptions to these policies: For instance, information can be accessed and preserved for an extended period when it is the subject of a legal request or obligation, governmental investigation, or investigations of possible violations of our terms or policies, or otherwise to prevent harm. We also retain information from accounts disabled for terms violations for at least a year to prevent repeat abuse or other term violations.

We collect very little data about non-users (unless they choose to communicate directly with us) and do not create profiles or track browsing history for people who are not registered users of Facebook, for example.

Particularly in the past few months, we've realized that we need to take a broader view of our responsibility to our community. Part of that effort is continuing our ongoing efforts to identify ways that we can improve our privacy practices. This includes restricting the way that developers can get information from Facebook and announcing plans to build Clear History, a new feature that will enable users to see the websites and apps that send us information when they use them, delete this information from their accounts, and turn off our ability to store it associated with their accounts going forward.

Question 7. Onavo Protect: When Facebook bought a VPN service, Onavo Protect, the purchase was portrayed as a way for your company to build more efficient mobile products. Since 2016, you have encouraged users to install the Onavo application as a way to "keep you and your data safe," although it does not brand itself as a Facebook product. Onavo is a particularly sensitive product since it provides your company access to all of the Internet traffic being generated by the device. Wall Street Journal and other publications have reported that Facebook has used the data captured from the Onavo for market analytics on competitive services.

Does Facebook use traffic information collected from Onavo to monitor the adoption or popularity of non-Facebook applications?

Answer. When people first install the *iOS version of the Onavo Protect app,* we explain that Onavo uses a VPN that "helps keep you and your data safe by understanding when you visit potentially malicious or harmful websites and giving you a warning." In addition, the first screen that a person sees when installing the app explains, under a heading that reads "Data Analysis":

> "When you use our VPN, we collect the info that is sent to, and received from, your mobile device. This includes information about: your device and its location, apps installed on your device and how you use those apps, the websites you visit, and the amount of data use.
>
> This helps us improve and operate the Onavo service by analyzing your use of websites, apps and data. Because we're a part of Facebook, we also use this info to improve Facebook products and services, gain insights into the products and services people value, and build better experiences."

People must tap a button marked "Accept & Continue" after seeing this information in a full-screen interstitial before they can use the app.

The Android version of the Onavo Protect app offers data management features (*e.g.,* the ability to block apps from using background data) that do not require users to enable the app's VPN.

For both versions of the app, we communicate repeatedly and up front—in the App Store description, in Onavo's Privacy Policy, and in-line at the time the user first opens the app after downloading it—that Onavo is part of Facebook and what that means for how Onavo Protect handles data in other ways.

More broadly, websites and apps have used market research services for years. We use Onavo, App Annie, comScore, and publicly available tools to help us understand the market and improve all our services. When people download Onavo to manage their data usage and help secure their connection, we are clear about the information we collect and how it is used. Like other VPNs, when the Onavo VPN is enabled, Onavo Protect helps create a secure connection, including when people are on public Wi-Fi. As part of this process, Onavo receives their mobile data traffic. This helps us improve and operate the Onavo service. Because we're part of Facebook, we also use this information to improve Facebook products and services. We let people know about this activity, and other ways that Onavo uses, analyzes, and shares data (for example, the apps installed on users' devices) in the App Store descriptions, and when they first open the app after downloading it.

Facebook does not use Onavo data for Facebook product uses, nor does it append any Onavo data or data about individuals' app usage to Facebook accounts.

Question 8. Has Facebook ever used the Onavo data in decisions to purchase another company or develop a product to compete against another company?

Answer. See Response to Question 7.

Question 9. Does Facebook associate Onavo traffic information with profile data from its social networking sites, including for analytic purposes?

Answer. See Response to Question 7.

Question 10. Facebook and Academic Research: Facebook's users place a significant amount of trust in the company to keep its data safe and protect the integrity of the platform. While Facebook has now developed a well-regarded ethical review processes and it is commendable that the company has supported academic research, any process is fallible and at least one of its experiments on "emotional contagion" was highly criticized by the academic community. One of the researchers behind the Cambridge Analytica application, Dr. Aleksandr Kogan, had frequently collaborated with Facebook on social science research based on its data, including a paper where Facebook provided data on every friendship formed in 2011 in every country in the world at the national aggregate level. Facebook users almost certainly are unaware that their data is used for scientific research by outside researchers nor do they have a credible understanding of the accountability of these relationships.

Has Facebook ever provided any third party researcher with direct access to non-anonymized user data?

Answer. In our Data Policy, we explain that we may use the information we have to conduct and support research in areas that may include general social welfare, technological advancement, public interest, health, and well-being. Researchers are subject to strict restrictions regarding data access and use as part of these collaborations.

Question 11. Do users have the ability to opt out of such experiments?

Answer. No, users do not have the ability to opt out of such research; however, we disclose our work with academic researchers in our Data Policy, and our work with academics is conducted subject to strict privacy and research protocols.

Question 12. Has a researcher ever been found to have misused access to the non-anonymized user data? Please describe any such incidents.

Answer. We are investigating all apps that, like Aleksandr Kogan's, had access to large amounts of information before we changed our platform in 2014 to reduce data access. The investigation process is in full swing, and it has two phases. First, a comprehensive review to identify every app that had access to this amount of Facebook data. And second, where we have concerns, we will conduct interviews, make requests for information (RFI)—which ask a series of detailed questions about the app and the data it has access to—and perform audits that may include on-site inspections. We have large teams of internal and external experts working hard to investigate these apps as quickly as possible. To date thousands of apps have been investigated and around 200 (from a handful of developers: Kogan, AIQ, Cube You, the Cambridge Psychometrics Center, and myPersonality) have been suspended—pending a thorough investigation into whether they did in fact misuse any data. Where we find evidence that these or other apps did misuse data, we will ban them and notify people whose data was shared with these apps. Additionally, we have suspended an additional 14 apps, which were installed by around one thousand people. They were all created after 2014, after we made changes to more tightly restrict our platform APIs to prevent abuse. However, these apps appear to be linked to AIQ, which was affiliated with Cambridge Analytica. So, we have suspended them while we investigate further. Any app that refuses to take part in or fails our audit will be banned.

Question 13. Does Facebook believe it would have a responsibility to report such incidents der the consent decree? If such incidents have occurred, has Facebook reported them to the FTC?

Answer. The July 27, 2012 Consent Order memorializes the agreement between Facebook and the FTC and does not require ongoing reporting.

Instead, and among other things, the consent order obligates Facebook not to misrepresent the extent to which it maintains the privacy or security of covered information (Section I), not to materially exceed the restrictions of a privacy setting that applies to nonpublic user information without affirmative express consent (Section II), and to implement a comprehensive privacy program that is subjected to ongoing review by an independent assessor (Sections IV and V). Facebook accurately represented the operation of its developer Platform and the circumstances under which people could share data (including friends data) with developers, honored the restrictions of all privacy settings that covered developer access to data, and implemented a comprehensive privacy program build on industry-leading controls and principles, which has undergone ongoing review by an independent assessor approved by the FTC.

Question 14. Cambridge Analytica Timeline Questions: There have been conflicting reports regarding the timeline of Facebook's response to the "thisisyourdigitallife" application developed for Cambridge Analytica. Please provide specific information about Facebook's response to the matter.

With respect to the harvesting of user data from the "thisisyourdigitallife" application, for each the following (a) Cambridge Analytica, (b) Christopher Wylie, and (c) Dr. Kogan, on what date did Facebook:

1. First contact that party about the data collected from the application?
2. Seek certification that the partys copy of the data was destroyed?
3. Receive the certification from party?

Answer. On December 11, 2015, *The Guardian* published an article reporting that Kogan and his company, GSR, may have passed information the app had obtained from Facebook users to SCL Elections Ltd. (SCL)/Cambridge Analytica. If this occurred, Kogan and his company violated Facebook's Platform Policies, which explicitly prohibited selling user data accessed from Facebook and from sharing any user data accessed from Facebook with any ad network, data broker or other advertising or monetization related service.

For this reason, Facebook immediately banned the app from our platform and investigated what happened and what further action we should take to enforce our Platform Policies. Facebook also contacted Kogan/GSR and demanded that they explain what data they collected, how they used it, and to whom they disclosed it. Facebook further insisted that Kogan and GSR, as well as other persons or entities to whom they had disclosed any such data, account for and irretrievably delete all such data and information.

Facebook also contacted Cambridge Analytica to investigate the allegations reflected in the reporting. On January 18, 2016, Cambridge Analytica provided written confirmation to Facebook that it had deleted the data received from Kogan and

that its server did not have any backups of that data. On June 11, 2016, Kogan executed and provided to Facebook signed certifications of deletion on behalf of himself and GSR. The certifications also purported to identify all of the individuals and entities that had received data from GSR (in addition to Kogan and his lab), listing the following: SCL, Eunoia Technologies (a company founded by Christopher Wylie), and a researcher at the Toronto Laboratory for Social Neuroscience at the University of Toronto. On July 7, 2016, a representative of the University of Toronto certified that it deleted any user data or user-derived data. On August 16, 2016, Eunoia (executed by Eunoia Founder Christopher Wylie) certified that it deleted any user and user-derived data. On September 6, 2016, counsel for SCL informed counsel for Facebook that SCL had permanently deleted all Facebook data and derivative data received from GSR and that this data had not been transferred or sold to any other entity. On April 3, 2017. Alexander Nix, on behalf of SCL, certified to Facebook, that it deleted the information that it received from GSR or Kogan.

Because all of these concerns relate to activity that took place off of Facebook and its systems, we have no way to confirm whether Cambridge Analytica may have Facebook data without conducting a forensic audit of its systems. Cambridge Analytica has agreed to submit to a forensic audit, but we have not commenced that yet due to a request from the UK Information Commissioner's Office, which is simultaneously investigating Cambridge Analytica (which is based in the UK). And even with an audit, it may not be possible to determine conclusively what data was shared with Cambridge Analytica or whether it retained data after the date it certified that data had been deleted.

The existing evidence that we are able to access supports the conclusion that Kogan only provided SCL with data on Facebook users from the United States. While the accounts of Kogan and SCL conflict in some minor respects not relevant to this question, both have consistently maintained that Kogan never provided SCL with any data for Facebook users outside the United States. These consistent statements are supported by a publicly released contract between Kogan's company and SCL.

Question 15. Was Facebook aware at that time that Cambridge Analytica had developed other platform applications to collect user data? What applications did it delete due to associations with Cambridge Analytica and when were they removed from the platform?

Answer. Our investigation of Cambridge Analytica's advertising activities is ongoing, and we have banned Cambridge Analytica from purchasing ads on our platform. Cambridge Analytica generally utilized custom audiences, some of which were created from contact lists and other identifiers that it generated and uploaded to our system to identify the people it wanted to deliver ads to on Facebook, and in some instances, refined those audiences with additional targeting attributes.

Question 16. Facebook's "People You May Know" Feature: Facebook's "People You May Know" feature has drawn attention for disclosures that reveal sensitive relationships, such as psychiatrists who have reported that their clients were recommended to each other.

What pieces of data does Facebook use for the PYMK feature? Has it ever used data collected from data brokers for this purpose?

Answer. People You May Know can help Facebook users find friends on Facebook. People You May Know suggestions come from things such as having friends in common, or mutual friends; being in the same Facebook group or being tagged in the same photo; users' networks (for example, school or work); and contacts users have uploaded. We give people context when we suggest someone with mutual friends. Users may delete contacts that they have uploaded to Facebook, in which case that information is no longer used for People You May Know. Facebook does not allow advertisers to target ads based o People You May Know. Facebook does not use data collected from data brokers for PYMK.

Question 17. Has PYMK ever used location to make recommendations and does it currently? If so, is this based on device reported geolocation or IP address?

Answer. PYMK uses country-level location to help users find friends.

Question 18. Does Facebook provide users with the ability to opt out of data collected from them or data about them being used by PYMK?

Answer. See Response to Question 16.

Question 19. Has the PYMK feature ever bypassed the privacy controls in order to perform its analytics for recommendations? For example, if a user's friends list is set to private, will Facebook still use this data to make recommendations to others?

Answer. See Response to Question 16.

Question 20. Other Cambridge Analyticas: Over a month ago, Mr. Zuckerberg stated that one of Facebook's next responsibilities was to "make sure that there aren't any other Cambridge Analyticas out there." One would expect that review process would include identifying past cases where Facebook identified or took action against third-party developers over their data collection practices.

When the company Klout automatically created accounts and assigned social popularity scores for the children of Facebook users, did Facebook send a deletion letter or exercise its right to audit?

Answer. In 2011, Facebook contacted Klout regarding potential violations of Facebook polices. Facebook determined that these issues had been resolved by Dec. 2011.

We use a variety of tools to enforce Facebook policies against violating parties, including developers. We review tens of thousands of apps per year and regularly disapprove noncompliant apps as part of our proactive review process. We also use tools like cease and desist letters, account suspensions, letter agreements, and civil litigation. For example, since 2006, Facebook has sent over 1,150 cease-and-desist letters to over 1,600 targets. In 2017, we took action against about 370,000 apps, ranging from imposing certain restrictions to removal of the app from the platform. Moreover, we have required parties who have procured our data without authorization to delete that data. We have invested significant resources in these efforts. Facebook is presently investigating apps that had access to large amounts of information before we changed our platform policies in 2014 to significantly reduce the data apps could access. To date around 200 apps (from a handful of developers: Kogan, AIQ, Cube You, the Cambridge Psychometrics Center, and myPersonality) have been suspended—pending a thorough investigation into whether they did in fact misuse any data.

Additionally, we have suspended an additional 14 apps, which were installed by around one thousand people. They were all created after 2014, after we made changes to more tightly restrict our platform APIs to prevent abuse. However, these apps appear to be linked to AIQ, which was affiliated with Cambridge Analytica. So, we have suspended them while we investigate further. Any app that refuses to take part in or fails our audit will be banned.

Question 21. How many times was Facebook made aware of privacy breaches by applications?

Answer. Facebook's policies regarding third-party usage of its platform technologies have prohibited—and continue to prohibit—those third-party app developers from selling or licensing user data obtained from Facebook and from sharing any user data obtained from Facebook with any ad network, data broker or other advertising or monetization-related service. We will investigate all apps that had access to large amounts of information before we changed our platform in 2014 to reduce data access, and we will conduct a full audit of any app with suspicious activity.

Question 22. How many times did Facebook send a deletion letter to an application developer for strictly privacy violations?

Answer. We use a variety of tools to enforce Facebook policies against violating parties, including developers. We review tens of thousands of apps per year and regularly disapprove noncompliant apps as part of our proactive review process. We also use tools like cease and desist letters, account suspensions, letter agreements, and civil litigation. For example, since 2006, Facebook has sent over 1,150 cease-and-desist letters to over 1,600 targets. In 2017, we took action against about 370,000 apps, ranging from imposing certain restrictions to removal of the app from the platform. Moreover, we have required parties who have procured our data without authorization to delete that data. We have invested significant resources in these efforts. Facebook is presently investigating apps that had access to large amounts of information before we changed our platform policies in 2014 to significantly reduce the data apps could access. To date around 200 apps (from a handful of developers: Kogan, AIQ, Cube You, the Cambridge Psychometrics Center, and myPersonality) have been suspended—pending a thorough investigation into whether they did in fact misuse any data.

Question 23. How many times did Facebook perform an audit on an application for strictly privacy violations?

Answer. See Response to Question 22.

Question 24. How many times did Facebook initiate litigation for strictly privacy violations?

Answer. See Response to Question 22.

Question 25. How many times did Facebook impose a moratorium or ban on an application developer for strictly privacy violations?

Answer. See Response to Question 22.

Question 26. Does Facebook plan to provide public disclosure of incidents where it finds that user data was improperly obtained or transferred by third-party application developers?

Answer. We are in the process of investigating every app that had access to a large amount of information before we changed our Platform in 2014. The investigation process is in full swing, and it has two phases. First, a comprehensive review to identify every app that had access to this amount of Facebook data and to focus on apps that present reason for deeper investigation. And second, where we have concerns, we will conduct interviews, make requests for information (RFI)—which ask a series of detailed questions about the app and the data it has access to—and perform audits using expert firms that may include on-site inspections. We have large teams of internal and external experts working hard to investigate these apps as quickly as possible. To date thousands of apps have been investigated and around 200 apps have been suspended—pending a thorough investigation into whether they did in fact misuse any data. Where we find evidence that these or other apps did misuse data, we will ban them and let people know.

These apps relate to a handful of developers: Kogan, AIQ, Cube You, the Cambridge Psychometrics Center, and myPersonality, with many of the suspended apps being affiliated with the same entity. Many of these suspensions include apps that appear to be "test" apps that were never released to the public, and therefore would not have acquired significant user data, although our investigation into these apps is ongoing.

Additionally, we have suspended an additional 14 apps, which were installed by around one thousand people. They were all created after 2014, after we made changes to more tightly restrict our platform APIs to prevent abuse. However, these apps appear to be linked to AIQ, which was affiliated with Cambridge Analytica. So, we have suspended them while we investigate further. Any app that refuses to take part in or fails our audit will be banned.

We will commit to briefing your staff on future developments.

Question 27. Facebook Privacy Settings: This month, Facebook began to roll out changes to comply with new European data protection rules. These updates include a new consent process that affects how Facebook uses sensitive data and whether facial recognition is enabled, among other factors.

Has Facebook engaged in user testing or other analysis that assessed how platform changes and interface design influence the adoption of certain privacy settings?

Answer. We routinely test new products and consent flows before rolling them out broadly to ensure that there are no bugs or unintended behaviors that would lead to an unintended or negative user experience. In designing the GDPR roll out, like all product roll outs, we rely on design principles and research derived from numerous sources, including user research and academic research, to develop experiences that are engaging and useful for the broadest number of people. We also conducted cross-disciplinary workshops, called "design jams," with experts around the world to collect input on user interaction principles that would inform our work. We have learned from our work and other design research in the field that people are less likely to make informed or thoughtful decisions when bombarded with many different choices in succession. To avoid so-called "notice fatigue," we streamlined the number of data choices people are presented with as part of the GDPR roll out to 2–3 choices (depending on the user's existing settings), responding to early testing of a version with several additional choices, which the people who tested this version did not like. We also used a layered approach that gave people the information needed to make an informed choice on the first screen, while enabling ready access to deeper layers of information and settings for those interested in a particular topic. We will continue to monitor how these and other privacy settings perform with users. It's important to us that people have the information they need to make the privacy choices that are right for them.

Question 28. Has Facebook ever tested platform changes and interface design to determine whether it would lead to users allowing more permissive privacy settings?

Answer. At Facebook, we make decisions about privacy through a cross-functional, cross-disciplinary effort that involves participants from departments across the company. This process is a collaborative approach to privacy that seeks to promote strong privacy protections and sound decision making at every stage of the product development process. Our privacy program is responsible for reviewing product launches, major changes, and privacy-related bug fixes to products and features to ensure that privacy policies and procedures are consistently applied and that key privacy decisions are implemented for the product. This approach has several key benefits.

First, it is designed to consider privacy early in the product development process. This allows us to consider the benefits that a feature is intended to have for people who use our services, how data will be used to deliver those benefits, and how we can build features from the ground up that include privacy protections to enable those benefits while protecting people's information and putting them in control.

Second, while complying with our obligations is critically important, taking a cross-disciplinary approach to privacy encourages us to think about data protection as more than just a compliance exercise. Instead, we evaluate how to design privacy into the features that we build and consider this from the perspective of things like how we design interfaces that make data use intuitive, taking a consistent approach to privacy across our services, and building protections in how our software is engineered. Accordingly, while we scale our privacy review process depending on the complexity of a particular data use, reviews typically involve experts who evaluate proposed data practices from the perspective of multiple disciplines.

As part of our consent agreement with the Federal Trade Commission, we submit a report to the FTC every two years. That report is based on assessments conducted by an independent third party on a bi-annual basis, which require us to submit evidence to demonstrate the effectiveness of the program.

Question 29. EU Data Protection Regulations: In Europe, under new data protection regulations, Facebook will be required to provide users will more clear opportunities to provide consent and afford more protections to that data. While Facebook has stated that it will offer some of those protections for users outside of Europe, it has not committed to providing all of these protection. I am interested in what rules Congress should put into place for such data.

Would Facebook support a requirement that users be provided with clear and plain information about the use of their data?

Answer. Yes. We work hard to provide clear information to people about how their information is used and how they can control it. We agree that companies should provide clear and plain information about their use of data and strive to do this in our Data Policy, in in-product notices and education, and throughout our product—and we continuously work on improving this. We provide the same information about our data practices to users around the world and are required under many existing laws—including U.S. laws (*e.g.,* Section 5 of the FTC Act) to describe our data practices in language that is fair and accurate.

Question 30. Would Facebook support a requirement that users be allowed to download and take their data to competitive services?

Answer. Facebook already allows users to download a copy of their information from Facebook. This functionality, which we've offered for many years, includes numerous categories of data, including About Me, Account Status History, Apps, Chat, Follower, Following, Friends, Messages, Networks, Notes, and more. We recently launched improvements to our "Download Your Information" tool, including to give people choices about whether they want to download only certain types of information and about the format in which they want to receive the download, to make it easier for people to use their information once they've retrieved it.

Question 31. Would Facebook support a requirement that users are assured that their data is actually deleted when they request its deletion or close their account?

Answer. In general, when a user deletes their account, we delete things they have posted, such as their photos and status updates, and they won't be able to recover that information later. (Information that others have shared about them isn't part of their account and won't be deleted.)

There are some limited exceptions to these policies: For instance, information can be accessed and preserved for an extended period when it is the subject of a legal request or obligation, governmental investigation, or investigations of possible violations of our terms or policies, or otherwise to prevent harm. We also retain information from accounts disabled for terms violations for at least a year to prevent repeat abuse or other term violations.

Question 32. Would Facebook support a requirement of mandatory and timely disclosure of breaches?

Answer. Facebook is generally open to the idea of breach notification requirements, particularly legislation that would centralize reporting and ensure a consistent approach across the United States. For example, in Europe, the GDPR requires notification to a lead supervisory authority, rather than individual member states, in cases of a data breach. In the United States, however, there is no centralized notification scheme, and instead, reporting obligations vary widely across all 50 states. This complexity makes it harder to respond appropriately and swiftly to protect people in the event of a data breach. We believe this is an important issue and an area that is ripe for thoughtful regulation.

Question 33. Would Facebook support a requirement for a baseline technical and organizational measures to ensure adequate data security?

Answer. Facebook is generally not opposed to regulation but wants to ensure it is the right regulation. The issues facing the industry are complex, multi-faceted, and affect an important part of peoples' lives. As such, Facebook is absolutely committed to working with regulators, like Congress, to craft the right regulations. Facebook would be happy to review any proposed legislation and provide comments.

Question 34. Russian Interference: As early as June 2015, the *New York Times Magazine* had documented the Internet Research Agency's interest in interfering with American politics, and even named specific Facebook accounts associated in the disinformation effort. The way that Facebook is designed, outsiders have very little insight into these efforts. And yet, the Russian media outlet RBC had identified accounts that were paying to spread content several months before Facebook took notice. *New York Times* also claims that as early as November 2016, Facebook's Chief Security Officer Alex Stamos had uncovered evidence that Russian operatives used the platform to weaponized information obtained from the hacking of the DNC and the Clinton campaign.

In a CNN interview, Mr. Zuckerberg for the first time disclosed that Facebook had found "a lot of different accounts coming from Macedonia" to spread false news during the Alabama special election. That election, another one decided by only small margin, was months ago. Mr. Zuckerberg acknowledged that Facebook expects there will be attempts to interfere in the midterm elections with newer tactics, a belief shared by the intelligence community.

Will you commit to providing Congress with information about disinformation and propaganda campaigns on a timely basis prior to the midterm elections?

Answer. We recently outlined steps we are taking on election integrity here: *https://newsroom.fb.com/news/2018/03/hard-questions-election-security/*.

Further, pursuant to the new transparency measures Facebook is launching, all advertisers who want to run ads with political content targeted at the U.S. will have to confirm their identity and location by providing either a U.S. driver's license or passport, last four digits of their social security number, and a residential mailing address. Ads that include political content and appear on Facebook or Instagram will include a "Paid for by" disclaimer provided by the advertisers that shows the name of the funding source for the ad.

Question 35. The *New York Times* reports details of Russian interference were removed from the April 2017 report "Information Operations and Facebook" by management due to political and business reasons. Will Facebook provide Congress with the original draft of the report?

Answer. In the run-up to the 2016 elections, we were focused on the kinds of cybersecurity attacks typically used by nation states, for example phishing and malware attacks. And we were too slow to spot this type of information operations interference. Since then, we've made important changes to prevent bad actors from using misinformation to undermine the democratic process.

This will never be a solved problem because we're up against determined, creative and well-funded adversaries. But we are making steady progress. Here is a list of the 10 most important changes we have made:

- *Ads transparency.* Advertising should be transparent: users should be able to see all the ads an advertiser is currently running on Facebook, Instagram, and Messenger. And for ads with political content, we've created an archive that will hold ads with political content for seven years—including information about ad impressions and spend, as well as demographic data such as age, gender, and location. People in Canada and Ireland can already see all the ads that a Page is running on Facebook—and we're launching this globally in June.
- *Verification and labeling.* Every advertiser will now need confirm their ID and location before being able to run any ads with political content in the U.S. All ads with political content will also clearly state who paid for them.
- *Updating targeting.* We want ads on Facebook to be safe and civil. We thoroughly criteria advertisers can use to ensure they are consistent with our principles. As a result, we removed nearly one-third of the targeting segments used by the IRA. We continue to allow some criteria that people may find controversial. But we do see businesses marketing things like historical books, documentaries or television shows using them in legitimate ways.
- *Better technology.* Over the past year, we've gotten increasingly better at finding and disabling fake accounts. We now block millions of fake accounts each day as people try to create them—and before they've done any harm. This is thanks to improvements in machine learning and artificial intelligence, which can

proactively identify suspicious behavior at a scale that was not possible before—without needing to look at the content itself.

- *Action to tackle fake news.* We are working hard to stop the spread of false news. We work with third party fact checking organizations to limit the spread of articles with rated false. To reduce the spread of false news, we remove fake accounts and disrupt economic incentives for traffickers of misinformation. We also use various signals, including feedback from our community, to identify potential false news. In countries where we have partnerships with independent third-party fact-checkers, stories rated as false by those fact-checkers are shown lower in News Feed. If Pages or domains repeatedly create or share misinformation, we significantly reduce their distribution and remove their advertising rights. We also want to empower people to decide for themselves what to read, trust, and share. We promote news literacy and work to inform people with more context. For example, if third-party fact-checkers write articles about a news story, we show them immediately below the story in the Related Articles unit. We also notify people and Page Admins if they try to share a story, or have shared one in the past, that's been determined to be false. In addition to our own efforts, we're learning from academics, scaling our partnerships with third-party fact-checkers, and talking to other organizations about how we can work together.
- *Significant investments in security.* We're doubling the number of people working on safety and security from 10,000 last year to over 20,000 this year. We expect these investments to impact our profitability. But the safety of people using Facebook needs to come before profit.
- *Industry collaboration.* Recently, we joined 34 global tech and security companies in signing a TechAccord pact to help improve security for everyone.
- *Information sharing and reporting channels.* In the 2017 German elections, we worked closely with the authorities there, including the Federal Office for Information Security (BSI). This gave them a dedicated reporting channel for security issues related to the Federal elections.
- *Tracking 40+ elections.* In recent months, we've started to deploy new tools and teams to proactively identify threats in the run-up to specific elections. We first tested this effort during the Alabama Senate election, and plan to continue these efforts for globe, including the U.S. midterms. Last year we used public service announcements to help inform people about fake news in 21 separate countries, including in advance of French, Kenyan and German elections.
- *Action against the Russia-based IRA.* In April, we removed 70 Facebook and 65 Instagram accounts—as well as 138 Facebook Pages—controlled by the IRA primarily targeted either at people living in Russia or Russian-speakers around the world including from neighboring countries like Azerbaijan, Uzbekistan, and Ukraine. The IRA has repeatedly used complex networks of inauthentic accounts to deceive and manipulate people in the U.S., Europe, and Russia—and we don't want them on Facebook anywhere in the world.

We are taking steps to enhance trust in the authenticity of activity on our platform, including increasing ads transparency, implementing a more robust ads review process, imposing tighter content restrictions, and exploring how to add additional authenticity safeguards.

Question 36. Hate Speech: Over the past months, human rights organizations and other civil society groups have raised attention to concerns over Facebook's insufficient response to hate speech in countries where there is a credible threat of violence. In addition to Myanmar, the *New York Times* recently published an article on how mob violence against Muslims in Sri Lanka was spurred by a baseless rumor that a Muslim restaurant owner was secretly feeding sterilization pills to women from the Sinhalese-Buddhist community.

Mr. Zuckerberg and other members of Facebook management have expressed a renewed commitment to providing resources to address these threats, including taking action to address those who generate hate speech. As Mr. Zuckerberg noted, AI will not be able to resolve such complex matters in the near or medium term, necessitating teams that deal with local languages and context. While Facebook currently has approximately 1,200 German content reviewers to comply with regulations, it only has plans to hire "dozens" of Burmese content reviewers. Hiring staff with reviewers, market specialists and analysts with the appropriate expertise can be difficult, but these reports of violence demonstrate the human cost of insufficient community resources to handle content and complaints.

What "specific product changes" will you be making to address hate speech in such countries? Will the new product changes enable content that violates Facebook's Community Standards to be removed within 24 hours?

Answer. We've been too slow to deal with the hate and violence in places like Myanmar and Sri Lanka. The challenges we face in a country that has fast come online are very different than those in other parts of the world, and we are investing in people, technology, and programs to help address them as effectively as possible.

We are increasing the number of Burmese and Sinhalese-language content reviewers as we continue to grow and invest in Myanmar and Sri Lanka. Our goal is always to have the right number of people with the right native language capabilities to ensure incoming reports are reviewed quickly and effectively. That said, there is more to tackling this problem than reported content. A lot of abuse may go unreported, which is why we are supplementing our hiring with investments in technology and programs.

We are building new tools so that we can more quickly and effectively detect abusive, hateful, or false content. We have, for example, designated several hate figures and organizations for repeatedly violating our hate speech policies, which has led to the removal of accounts and content that support, praise, or represent these individuals or organizations. We are also investing in artificial intelligence that will help us improve our understanding of dangerous content.

We are further strengthening our civil society partner network so that we have a better understanding of local context and challenges. We are focusing on digital literacy education with local partners in Myanmar and Sri Lanka. For example, we launched a local language version of our Community Standards (*https://www.facebook.com/safety/resources/myanmar*) to educate new users on how to use Facebook responsibly in 2015 and we have been promoting these actively in Myanmar, reaching over 8 million people through promotional posts on our platform alone. We've also rolled out several education programs and workshops with local partners to update them on our policies and tools so that they can use this information in outreach to communities around the country. One example of our education initiatives is our work with the team that developed the Panzagar initiative (*https://www.facebook.com/supportflowerspeech*) to develop the Panzagar counter-speech Facebook stickers to empower people in Myanmar to share positive messages online. We also recently released locally illustrated false news tips, which were promoted on Facebook and in consumer print publications. We have a dedicated Safety Page for Myanmar (*https://www.facebook.com/safety/resources/myanmarand*) and have delivered hard copies of our local language Community Standards and safety and security tips to civil society groups in Myanmar who have distributed them around the country for trainings. Similarly, in Sri Lanka, we ran a promotion in English, Sinhalese, and Tamil at the top of News Feeds in April 2017 to educate people on our Community Standards, in particular hate speech. The content has been viewed almost 100M times by almost 4M people.

Question 37. Does Facebook believe that it has hired or will hire within the year a sufficient number of content reviewers and established local emergency points of contact for all regions where its platform could inadvertently facilitate communal violence?

Answer. We are investing in people, technology, and programs to help address the very serious challenges we have seen in places like Myanmar and Sri Lanka.

Our content review teams around the world—which grew by 3,000 people last year—work 24 hours a day and in over 50 languages.

Over the last two years, we have added dozens more Burmese language reviewers to handle reports from users across our services, and we plan to more than double the number of content reviewers focused on user reports. We also have increased the number of people across the company working on Myanmar-related issues and we have a special product team working to better understand the local challenges and build the right tools to help keep people in the country safe. We will continue to hire more staff dedicated to Myanmar, including Burmese speakers and policy experts.

In Sri Lanka, we are increasing the number of Sinhalese language experts sevenfold. From a programmatic perspective, we will continue to work with experts to develop safety resources and counter-speech campaigns in these regions and conduct regular training for civil society and community groups on using our tools.

Facebook is committed to continuing to provide a platform where people can raise awareness about human rights abuses around the globe, and we have a track record of partnering with experts and local organizations on these issues. For example, we have been part of the Global Network Initiative (GNI) since 2013. That organization brings together industry, civil society, academics, and socially-responsible investors to address freedom-of-expression and privacy issues online. An independent assessor

conducted a human-rights-impact assessment of Facebook to confirm that we comply with GNI's principles.

Question 38. What product changes, operational decisions, and resource allocations has Facebook made in order to avoid future risks such as those made abundantly clear in Myanmar and Sri Lanka?

Answer. We are working to enable freedom of expression around the globe and ensure that our platform is safe. Our Community Standards account for situations in which people may be raising awareness of and/or condemning violence; however, they prohibit hate speech and celebrating graphic violence. Drawing that line can be complex, which is why we work with experts and external groups, including local civil society organizations in places like Myanmar and Sri Lanka, to ensure that we are taking local context and challenges into account. Our content review team, which includes native language speakers, carefully reviews reports that we receive from the public, media, civil society, and governments. We remove content that violates our policies, regardless of who posted the content (including the government). We have also been working with local communities and NGOs for years in these regions to educate people about hate speech, news literacy, and our polices. For example, we have introduced an illustrated, Myanmar language specific copy of our community standards and a customized safety Page, which we work with our local partners to promote, and we recently ran a series of public service ads in Myanmar that we developed with the News Literacy Project to help inform people about these important issues.

Question 39. What emergency processes for escalation do you have in place for situations where there is content inciting people to violence, such as what happened in Sri Lanka?

Answer. We have clear rules against hate speech and content that incites violence, and we remove such content as soon as we're made aware of it. In response to the situation in Sri Lanka, we're building up teams that deal with reported content, working with civil society and government to learn more about local context and changing language, and exploring the use of technology to help. We want to provide direct reporting channels to civil society partners so that they can alert us to offline activity that might prompt an increase in violating content on Facebook. We work with local civil society organizations to understand what types of reporting channels would best serve their specific communities and are engaging with organizations in Sri Lanka to understand what more we can do. We are committed to having the right policies, products, people, and partnerships in place to help keep our community in Sri Lanka safe.

Question 40. In the context of Sri Lanka and Myanmar, rumors present a credible threat of violence and have resulted in violence. Are rumors such as those in Sri Lanka interpreted as violations under your existing "credible threat" policy? How do your systems or reporting mechanisms account for such country or context specific threats? Given how quickly such content can lead to violence, do you apply different processes or response time targets to prioritize content categorized as hate speech?

Answer. We require everyone on Facebook to comply with our Community Standards, and we carefully review reports of threatening language to identify serious threats of harm to public and personal safety. We recognize our services have an important role to play in countries that are fast coming online. That's why we're investing in people, technology, and programs to address the challenges we face in these countries. We've added more local language reviewers, established dedicated product teams, rolled out better reporting tools and appeals, and are removing fake accounts, hate groups and individuals. We remove credible threats of physical harm to individuals and specific threats of theft, vandalism, or other financial harm. We also prohibit the use of Facebook to facilitate or organize criminal activity that causes physical harm to people, businesses or animals, or financial damage to people or businesses, and we work with law enforcement when we believe there is a genuine risk of physical harm or direct threats to public safety. As part of our work in places like Sri Lanka and Myanmar, we are strengthening our relationships with civil society organizations to ensure we are taking local context, challenges, and tensions into account.

Question 41. The anti-Muslim monk, U Wirathu, was reportedly banned by Facebook in January 2018 after having been frequently reported for hate content. Despite several bans, he was able to recreate a presence on the platform on several occasions and there are to this day accounts which carry his name. What mechanisms do you have in place to remove users who repeatedly breach Facebook's Community Standards and what actions are you taking to guarantee their permanent removal?

Answer. Our Community Standards (*https://www.facebook.com/communitystandards*) prohibit hate speech that targets people based on their race, ethnic identity, or religion. We remove violating content when it is reported to us. We also have designated several hate figures and hate organizations in Myanmar. These include Wirathu, Thuseitta, Ma Ba Tha, and Parmaukkha. This means these individuals or organizations are not allowed a presence on Facebook, and we will remove accounts and content that support, praise or represent these individuals or organizations.

In addition to removing content that violates our Community Standards or Page Terms, we disable the accounts of repeat infringers in appropriate circumstances.

Over the last several months, we have proactively searched for and removed content on the platform that praises, supports, or represents Wirathu.

Question 42. Human Rights—Iran: Iranian women's rights and pro-democracy advocates have reported that copyright infringement and content reporting mechanisms have been instrumentalized by pro-government actors to take down their Instagram pages and Facebook Groups over the past several years. While community reporting mechanisms are necessary, and often legally required, for operating a platform as large as Facebook, the threat posed by abusive reporting also demonstrates the need for human reviewers. Likewise, the trolling, hacking, and impersonation that frequently target Iranian dissidents also necessitate teams that are empowered to deal with the Persian language and the Iranian context. However, many activists have struggled to establish relationships or receive help from Facebook to have such issues addressed.

Answer. We recognize that individuals and entities may purposefully report content en masse in an attempt to stifle speech. That is why we believe content must be reviewed with the appropriate context.

We are proud that our platform has been used to inspire people to stand up for their beliefs and values, even in the face of intimidating opposition, and we regularly provide tools and programmatic resources to activists and journalists. We also make materials available to ensure activists and journalists are able to use Facebook safely.

Based on the foundation established in the Universal Declaration of Human Rights and the UN Guiding Principles on Business and Human Rights, Facebook joined the ICT-sector specific Global Network Initiative in 2013. As part of our commitments as a GNI member, we routinely conduct human rights impact assessments of our product and policy decisions and engage with external stakeholders to inform this work. We are also independently assessed against our compliance with the GNI Principles every two years.

Question 43. What measures, such as verification of accounts, has Facebook taken to address the impersonation of Iranian activists, cultural dissidents, and other public figures?

Answer. Claiming to be another person violates our Community Standards, and we want to make it harder for anyone to be impersonated on our platform. Users can also report accounts that are impersonating them. We've developed several techniques to help detect and block this type of abuse. At the time someone receives a friend request, our systems are designed to check whether the recipient already has a friend with the same name, along with a variety of other factors that help us determine if an interaction is legitimate. Further, we recently announced new features that use face recognition technology that may help detect when someone is using another user's image as their profile photo—which helps stop impersonation. This is an area we're continually working to improve so that we can provide a safe and secure experience on Facebook.

RESPONSE TO WRITTEN QUESTIONS SUBMITTED BY HON. BRIAN SCHATZ TO MARK ZUCKERBERG

Question 1. You said at the hearing that Facebook users own and control their data. But I am not persuaded that the company has done an adequate job explaining, for example, what specific information the company collects about individuals, how that information is being used and kept safe, and how they can easily delete or modify it. If you and your company are committed to putting privacy first, I urge that you answer these questions in a precise, accurate, but straightforward way. I understand your legal team will be reviewing this, but I hope you resist complexity and answer these questions in a way that any American could understand.

Please list and describe all of the types and categories of data that Facebook collects and how Facebook uses this data. This includes, but is not limited to, data collected:

- on the Facebook platform (*e.g.,* posts, messages, and search history);
- off the Facebook platform (quantify how ubiquitous Facebook's plugins are on the web, for instance);
- on products offered by Facebook family companies;
- on specific devices (*e.g.,* smartphone microphone and camera, other apps, data from the operating system);
- via third-party companies and app developers;
- from data brokers; and
- from publishers.

For each, describe whether users own the data, and what options users have to modify or delete the data.

Answer. We believe that it's important to communicate with people about the information that we collect and how people can control it. That is why we work hard to provide this information to people in a variety of ways: in our Data Policy, and in Privacy Basics, which provides walkthroughs of the most common privacy questions we receive. Beyond simply disclosing our practices, we also think it's important to give people access to their own information, which we do through our Download Your Information and Access Your Information tools, Activity Log, and Ad Preferences, all of which are accessible through our Privacy Shortcuts tool. We also provide information about these topics as people are using the Facebook service itself.

We've heard loud and clear that privacy settings and other important tools are too hard to find and that we must do more to keep people informed. So, we're taking additional steps to put people more in control of their privacy. For instance, we redesigned our entire settings menu on mobile devices from top to bottom to make things easier to find. We also created a new Privacy

Shortcuts in a menu where users can control their data in just a few taps, with clearer explanations of how our controls work. The experience is now clearer, more visual, and easy-to-find. Furthermore, we also updated our terms of service that include our commitments to everyone using Facebook. We explain the services we offer in language that's easier to read. We're also updating our Data Policy to better spell out what data we collect and how we use it in Facebook, Instagram, Messenger, and other products.

In response to your specific questions, depending on which Services a person uses, we collect different kinds of information from or about them. This is described in our Data Policy:

- *Things Users and others do and provide.* Information and content users provide. We collect the content, communications and other information users provide when they use our Products, including when they sign up for an account, create or share content, and message or communicate with others. This can include information in or about the content they provide (like metadata), such as the location of a photo or the date a file was created. It can also include what users see through features we provide, such as our camera, so we can do things like suggest masks and filters that they might like, or give users tips on using camera formats. Our systems automatically process content and communications users provide to analyze context and what's in them for the purposes described below. Learn more about how people can control who can see the things they share.
    - Data with special protections: Users can choose to provide information in their Facebook profile fields or Life Events about their religious views, political views, who they are "interested in," or their health. This and other information (such as racial or ethnic origin, philosophical beliefs, or trade union membership) could be subject to special protections under the laws of their country.
- *Networks and connections.* We collect information about the people, Pages, accounts, hashtags, and groups users are connected to and how they interact with them across our Products, such as people a user communicates with the most or groups users are part of. We also collect contact information if they choose to upload, sync, or import it from a device (such as an address book or call log or SMS log history), which we use for things like helping them and others find people they may know and for the other purposes listed below.
- *People's usage.* We collect information about how people use our Products, such as the types of content they view or engage with; the features they use; the actions they take; the people or accounts they interact with; and the time, frequency, and duration of their activities. For example, we log when they're using

and have last used our Products, and what posts, videos, and other content they view on our Products. We also collect information about how they use features like our camera.

- *Information about transactions made on our Products.* If people use our Products for purchases or other financial transactions (such as when users make a purchase in a game or make a donation), we collect information about the purchase or transaction. This includes payment information, such as their credit or debit card number and other card information; other account and authentication information; and billing, shipping, and contact details.
- *Things others do and information they provide about users.* We also receive and analyze content, communications, and information that other people provide when they use our Products. This can include information about them, such as when others share or comment on a photo of a user, send a message to them, or upload, sync or import their contact information.
- *Device Information.* As described below, we collect information from and about the computers, phones, connected TVs and other web-connected devices they use that integrate with our Products, and we combine this information across different devices they use. For example, we use information collected about their use of our Products on their phone to better personalize the content (including ads) or features they see when they use our Products on another device, such as their laptop or tablet, or to measure whether they took an action in response to an ad we showed they on their phone on a different device.

Information we obtain from these devices includes:

  - Device attributes: information such as the operating system, hardware and software versions, battery level, signal strength, available storage space, browser type, app and file names and types, and plugins.
  - Device operations: information about operations and behaviors performed on the device, such as whether a window is foregrounded or backgrounded, or mouse movements (which can help distinguish humans from bots).
  - Identifiers: unique identifiers, device IDs, and other identifiers, such as from games, apps or accounts people use, and Family Device IDs (or other identifiers unique to Facebook Company Products associated with the same device or account).
  - Device signals: Bluetooth signals, and information about nearby Wi-Fi access points, beacons, and cell towers.
  - Data from device settings: information users allow us to receive through device settings people turn on, such as access to their GPS location, camera, or photos.
  - Network and connections: information such as the name of users' mobile operator or ISP, language, time zone, mobile phone number, IP address, connection speed and, in some cases, information about other devices that are nearby or on users' network, so we can do things like help people stream a video.
  - Cookie data: data from cookies stored on a user's device, including cookie IDs and settings. Learn more about how we use cookies in the Facebook Cookies Policy (*https://www.facebook.com/policies/cookies/*) and Instagram Cookies Policy (*https://www.instagram.com/legal/cookies/*).

- *Information from partners.* Advertisers, app developers, and publishers can send us information through Facebook Business Tools they use, including our social plug-ins (such as the Like button), Facebook Login, our APIs and SDKs, or the Facebook pixel. These partners provide information about users' activities off Facebook—including information about a user's device, websites users visit, purchases users make, the ads they see, and how they use their services—whether or not they have a Facebook account or are logged into Facebook. For example, a game developer could use our API to tell us what games users play, or a business could tell us about a purchase a user made in its store. We also receive information about a user's online and offline actions and purchases from third-party data providers who have the rights to provide us with their information. Partners receive user data when users visit or use their services or through third parties they work with. We require each of these partners to have lawful rights to collect, use and share user data before providing any data to us.

People own what they share on Facebook, and they can manage things like who sees their posts and the information they choose to include on their profile.

Any person can see each of the specific interests we maintain about them for advertising by visiting Ads Preferences, which lets people see what interests we use to choose ads for them—and to edit or delete these interests. They can choose not to see ads from a particular advertiser or not to see ads based on their use of third-party websites and apps. They also can choose not to see ads off Facebook that are based on the interests we derive from their activities on Facebook.

Our Download Your Information or "DYI" tool is Facebook's data portability tool and was launched many years ago to let people access and download many types of information that we maintain about them. The data in DYI and in our Ads Preferences tool contain each of the interest categories that are used to show people ads, along with information about the advertisers are currently running ads based on their use of an advertiser's website or app. People also can choose not to see ads from those advertisers. We recently announced expansions to Download Your Information, which, among other things, will make it easier for people to see their data, delete it, and easily download and export it. More information is available at *https://newsroom.fb.com/news/2018/04/new-privacy-protections/*.

And we recently announced plans to build Clear History. This feature will enable users to see the websites and apps that send us information when they use them, delete this information from their accounts, and turn off our ability to store it associated with their accounts going forward. Apps and websites that use features such as the Like button or Facebook Analytics send us information to make their content and ads better. We also use this information to make users' experiences on Facebook better. If a user clears their history or use the new setting, we'll remove identifying information so a history of the websites and apps they've used won't be associated with their account. We'll still provide apps and websites with aggregated analytics—for example, we can build reports when we're sent this information so we can tell developers if their apps are more popular with men or women in a certain age group. We can do this without storing the information in a way that's associated with a user's account, and as always, we don't tell advertisers who a user is.

Question 2. What data does Facebook collect about non-users? For example, when a user first joins Facebook, what data has Facebook already typically collected about them? Assume that the new user is an average American and active web user with many friends who are already on Facebook. List the attributes that Facebook would typically know about the new user and where that information comes from. If Facebook collects information about non-users, what is the purpose?

Answer. Facebook does not create profiles or track website visits for people without a Facebook account.

When people visit apps or websites that feature our technologies—like the Facebook Like or Comment button—our servers automatically log (i) standard browser or app records of the fact that a particular device or user visited the website or app (this connection to Facebook's servers occurs automatically when a person visits a website or app that contains our technologies, such as a Like button, and is an inherent function of Internet design); and (ii) any additional information the publisher of the app or website chooses to share with Facebook about the person's activities on that site (such as the fact that a purchase was made on the site). This is a standard feature of the Internet, and most websites and apps share this same information with multiple different third-parties whenever people visit their website or app. For example, the Senate Commerce Committee's website shares information with Google and its affiliate DoubleClick and with the analytics company Webtrends. This means that, when a person visits the Committee's website, it sends browser information about their visit to each one of those third parties. More information about how this works is available at *https://newsroom.fb.com/news/2018/04/data-off-facebook/*.

When the person visiting a website featuring Facebook's tools is not a registered Facebook user, Facebook does not have information identifying that individual, and it does not create profiles for this individual.

We use the browser and app logs that apps and websites send to us—described above—in the following ways for non-Facebook users. First, these logs are critical to protecting the security of Facebook and to detecting or preventing fake account access. For example, if a browser has visited hundreds of sites in the last five minutes, that's a sign the device might be a bot, which would be an important signal of a potentially inauthentic account if that browser then attempted to register for an account. Second, we aggregate those logs to provide summaries and insights to websites and apps about how many people visit or use their product or use specific features like our Like button—but without providing any information about a specific person. We do not create profiles for non-Facebook users, nor do we use browser and app logs for non-Facebook users to show targeted ads from our advertisers to them or otherwise seek to personalize the content they see. However, we may take

the opportunity to show a general ad that is unrelated to the attributes of the person or an ad encouraging the non-user to sign up for Facebook.

Question 3. Last year, how many Facebook users clicked on their privacy settings at least once? What was the average time a user spent adjusting their privacy controls? How often does an average user go into their privacy settings (per year, for instance)? In 2017, how many times did Facebook modify the user experience of its privacy settings to better suit its users? What other analytics of this kind does Facebook measure?

Answer. Privacy is at the core of everything we do, and our approach to privacy starts with our commitment to transparency and control. Our threefold approach to transparency includes, first, whenever possible, providing information on the data we collect and use and how people can control it in context and in our products. Second, we provide information about how we collect and use data in our user agreements and related educational materials. And third, we enable people to learn more about the specific data we have about them through interactive tools such as Download Your Information, which lets people download a file containing data that they may want to take to another service, and Access Your Information, a tool we are launching that will let people more easily access and manage their data on Facebook.

Our approach to control is based on the belief that people should be able to choose who can see what they share and how their data shapes their experience on Facebook. People can control the audience for their posts and the apps that can receive their data. They can see and delete the history of their activities on Facebook, and, if they no longer want to use Facebook, they can delete their account and the data associated with it. Of course, we recognize that controls are only useful if people know how to find and use them. That is why we continuously deliver in-product educational videos in people's News Feeds on important privacy topics. We are also inviting people to take our Privacy Checkup—which prompts people to review key data controls—and we are sharing privacy tips in education campaigns off of Facebook, including through ads on other websites. To make our privacy controls easier to find, we are launching a new settings menu that features core privacy settings in a single place. We are always working to help people understand and control how their data shapes their experience on Facebook.

Question 4. At the hearing, you said that you don't believe that enough users read Facebook's terms-of-service policy. Facebook has some of tech's smartest UX and behavioral experts, which is evident by a platform that millions of people use for hours each week. How is Facebook applying its UX and behavioral expertise to track and improve user engagement in this area? What does Facebook know about its users' understanding of its terms-of-service? For example, how long do users take to read Facebook's policies, on average? What does this number indicate about whether users have actually read the material?

Answer. We believe that it's important to communicate with people about the information that we collect and how people can control it. This is why we work hard to provide this information to people in a variety of ways: in our Data Policy, and in Privacy Basics, which provides walkthroughs of the most common privacy questions we receive. Beyond simply disclosing our practices, we also think it's important to give people access to their own information, which we do through our Download Your Information and Access Your Information tools, Activity Log, and Ad Preferences, all of which are accessible through our Privacy Shortcuts tool. We also provide information about these topics as people are using the Facebook service itself.

As to your specific question, there is no single number that measures how much time people spend understanding how Facebook services work, in large part because Facebook seeks, as much as possible, to put controls and information in context within its service. While "up front" information like that contained in the terms of service are useful, research overwhelmingly demonstrates that in-product controls and education are the most meaningful to people and the most likely to be read and understood. On-demand controls are also important, and we recently redesigned our entire settings menu on mobile devices from top to bottom to make things easier to find. We also created a new Privacy Shortcuts, a menu where people can control their data in just a few taps, with clearer explanations of how our controls work. The experience is now clearer, more visual, and easy-to-find.

Improving people's understanding of how digital services work is an industry-wide challenge that we are highly committed to addressing. That's why, over the last 18 months, we've run a global series of design workshops called "Design Jams", bringing together experts in design, privacy, law, and computer science to work collaboratively on new and innovative approaches. These workshops have run in Paris, London, Dublin, Berlin, Sao Paolo, Hong Kong, and other cities, and included global

regulators and policymakers. At these workshops, expert teams use "people centric design" methods to create innovative new design prototypes and experiences to improve transparency and education in digital services. These workshops inform Facebook's constantly-improving approach.

In recognition of the need for improved approaches to data transparency across all digital services, working with partners from academia, design, and industry we recently launched TTC Labs, a design innovation lab that seeks to improve user experiences around personal data. TTC Labs is an open platform for sharing and innovation and contains insights from leading experts in academia, design, and law, in addition to prototype designs from the design jams, template services and open-source toolkits for people-centric design for transparency, trust and control of data. Working collaboratively, and based on open-source approaches, TTC Labs seeks to pioneer new and more people-centric best practices for people to understand how their data is used by digital services, in ways that they find easy to understand and control.

Facebook is highly committed to improving people's experience of its own services as well as investing in new innovations and approaches to support improvements across the industry.

Question 5. Recently you said Facebook would "make all controls and settings the same everywhere, not just in Europe." Please describe these controls and settings and what they do? Would the modification of these controls and settings apply in the U.S. only to new users or to all users? Would Facebook commit to default those settings and controls to minimize, to the greatest extent, the collection and use of users' data? What changes will U.S. users see in their settings and controls after this change is implemented? And what features and protections (including but not limited to controls and settings) will European Facebook users have that will differ from U.S. users after the company implements GDPR?

Answer. The GDPR requires companies to obtain explicit consent to process certain kinds of data ("special categories of data" like biometric data). We are seeking explicit consent from people in Europe to three specific uses of data: facial recognition data (which previously was not enabled in Europe), special categories of data and use of data we collect off Facebook Company Products to target ads. We recently began providing direct notice of these controls and our updated terms to people around the world (including in the U.S.), allowing people to choose whether or not to enable or disable these settings or to agree to our updated terms. Outside of Europe we are not requiring people to complete those flows if they repeatedly indicate that they do not want to go through the experience. At the same time, the events of recent months have underscored how important it is to make sure people know how their information is used and what their choices are. So, we decided to communicate prominently on Facebook—through a full-screen message and a reminder to review at a later date. People can choose to dismiss or ignore these messages and continue using Facebook.

The controls and settings that Facebook is enabling as part of GDPR are already available to other users around the world, including in the U.S.. We also provide identical levels of transparency in our user agreements and in product notices to people in the U.S. that we are providing under GDPR.

In the U.S., where these settings are already in place, people will have a mechanism to maintain their current choice or to change it. In each of these cases, we want people to make the choice—not Facebook—so nobody's settings will change as part of this roll out unless they choose to change an existing setting.

And we also provide the same tools for access, rectification, erasure, data portability and others to users in in the U.S. and rest of world that we provide in Europe, and many of those tools (like our Download Your Information tool, Ads Preferences tool, and Activity Log) have been available globally for many years.

RESPONSE TO WRITTEN QUESTIONS SUBMITTED BY HON. EDWARD MARKEY TO MARK ZUCKERBERG

Question 1. Mr. Zuckerberg, your company has stated that it has "no plans" to include advertisements on Messenger Kids. Will you pledge that Facebook will never incorporate advertising into Messenger Kids or any future products for children 12 and under?

Answer. We have no plans to include advertising in Messenger Kids. Moreover, there are no in-app purchases, and we do not use the data in Messenger Kids to advertise to kids or their parents. In developing the app, we assembled a committee of advisors, including experts in child development, online safety, and media and children's health, and we continue to work with them on an ongoing basis. In addi-

tion, we conducted roundtables with parents from around the country to ensure we were addressing their concerns and built the controls they need and want in the app. We are committed to approaching all efforts related to children 12 and under thoughtfully, and with the guidance and input of experts and parents.

Question 2. In your response to my letter on the topic of Messenger Kids, you stated that your company will not "automatically" create a Facebook account for Messenger Kids users when those children turn 13. Will you commit to not share children's information for targeted advertisements, once young users turn 13?

Answer. As we stated in our response to your earlier letter, we will not automatically create a Facebook account for Messenger Kids users, or automatically transition a Messenger Kids account into a Facebook account once a child turns 13. Contained within that commitment and our commitment not to use data collected within Messenger Kids to market to kids or their parents is a commitment that we will not automatically enable third parties to send targeted ads to children who have used Messenger Kids when the child turns 13.

RESPONSE TO WRITTEN QUESTIONS SUBMITTED BY HON. TOM UDALL TO MARK ZUCKERBERG

Question 1. Data Protection on Facebook: The General Data Protection Regulation or "GDPR", which will go into effect on May 25 of this year. Will Facebook provide the same privacy protections for consent, retention, data portability, and transparency to American consumers that it will provide to EU consumers?

Answer. The controls and settings that Facebook is enabling as part of GDPR are available to people around the world, including settings for controlling our use of face recognition on Facebook and for controlling our ability to use data we collect off Facebook Company Products to target ads. We recently began providing direct notice of these controls and our updated terms to people around the world (including in the U.S.), allowing people to choose whether or not to enable or disable these settings or to consent to our updated terms. We provide the same tools for access, rectification, erasure, data portability and others to people in the U.S. and rest of world that we provide in Europe, and many of those tools (like our Download Your Information tool, ad preferences tool, and Activity Log) have been available globally for many years. We also provide identical levels of transparency in our user agreements and in product notices to people in the United States that we are providing under GDPR.

Question 2. What kind of privacy review is required to make a change to Facebook that impacts user privacy? When did that level of review become mandatory?

Answer. At Facebook, we make decisions about privacy through a cross-functional, cross-disciplinary effort overseen by the Chief Privacy Officer that involves participants from departments across the company. This process is a collaborative approach to privacy that seeks to promote strong privacy protections and sound decision making at every stage of the product development process. Our privacy program is responsible for reviewing product launches, major changes, and privacy-related bug fixes to products and features to ensure that privacy policies and procedures are consistently applied and that key privacy decisions are implemented for the product. This approach has several key benefits:

- First, it is designed to consider privacy early in the product development process. This allows us to consider the benefits that a feature is intended to have for people who use our services, how data will be used to deliver those benefits, and how we can build features from the ground up that include privacy protections to enable those benefits while protecting people's information and putting them in control.
- Second, while complying with our obligations is critically important, taking a cross-disciplinary approach to privacy encourages us to think about data protection as more than just a compliance exercise. Instead, we evaluate how to design privacy into the features that we build and consider this from the perspective of things like how we design interfaces that make data use intuitive, taking a consistent approach to privacy across our services, and building protections in how our software is engineered. Accordingly, while we scale our privacy review process depending on the complexity of a particular data use, reviews typically involve experts who evaluate proposed data practices from the perspective of multiple disciplines.

As part of our consent agreement with the Federal Trade Commission, we submit a report to the FTC every two years. That report is based on assessments conducted

by an independent third party on a bi-annual basis, which require us to submit evidence to demonstrate the effectiveness of the program.

Question 3. Before that level of review was required, what checks were in place to ensure new features would not adversely impact users' privacy? What level of seniority was required of employees to approve a launch of such a privacy-impacting feature? For example, have you ever allowed an intern make changes that impacts customers' privacy?

Answer. See Response to Question 2.

Question 4. Has Facebook ever launched a feature that had to be turned off because of the privacy concerns? If yes, how many times has that happened, and how many users were impacted? Did you notify the users who were impacted?

Answer. See Response to Question 2.

Question 5. Russia/Cambridge Analytica: Between 2010 and 2015, 3rd party applications were able to keep data indefinitely. Can you say how many applications downloaded app users' data, their friends' data, or their personal messages in this period of time?

Answer. We are in the process of investigating every app that had access to a large amount of information before we changed our Platform in 2014. The investigation process is in full swing, and it has two phases. First, a comprehensive review to identify every app that had access to this amount of Facebook data and to focus on apps that present reason for deeper investigation. And second, where we have concerns, we will conduct interviews, make requests for information (RFI)—which ask a series of detailed questions about the app and the data it has access to—and perform audits using expert firms that may include on-site inspections. We have large teams of internal and external experts working hard to investigate these apps as quickly as possible. To date thousands of apps have been investigated and around 200 apps have been suspended—pending a thorough investigation into whether they did in fact misuse any data. Where we find evidence that these or other apps did misuse data, we will ban them and let people know.

These apps relate to a handful of developers: Kogan, AIQ, Cube You, the Cambridge Psychometrics Center, and myPersonality, with many of the suspended apps being affiliated with the same entity. Many of these suspensions include apps that appear to be "test" apps that were never released to the public, and therefore would not have acquired significant user data, although our investigation into these apps is ongoing.

Additionally, we have suspended an additional 14 apps, which were installed by around one thousand people. They were all created after 2014, after we made changes to more tightly restrict our platform APIs to prevent abuse. However, these apps appear to be linked to AIQ, which was affiliated with Cambridge Analytica. So, we have suspended them while we investigate further. Any app that refuses to take part in or fails our audit will be banned.

We will commit to briefing your staff on future developments.

Question 6. Given the recent reports about Cambridge Analytica and the years of poor security around your data, what measures will be put into place to ensure that advertisers are not targeting ads using ill-gotten data?

Answer. We are not aware of any evidence to suggest that Kogan shared data obtained through his app with Russia or other foreign governments, but our investigation is ongoing. We are in the process of investigating every app that had access to a large amount of information before we changed our Platform in 2014.

In April 2014, we significantly restricted the types of data generally available to app developers and required apps seeking additional categories of data to undergo proactive review by our internal teams. We rejected more than half of the apps seeking these permissions, including the second version of Kogan's app.

We review apps to ensure that the requested permissions clearly improve the user experience and that the data obtained is tied to an experience within the app. We conduct a variety of manual and automated checks of applications on the platform for Policy compliance, as well as random sampling. When we find evidence of or receive allegations of violations, we investigate and, where appropriate, employ a number of measures, including restricting applications from our platform, preventing developers from building on our platform in the future, and taking legal action where appropriate.

Recently, we announced a number of additional steps we're taking to address concerns raised by Kogan's app.

- *Review our platform.* We will investigate all apps that had access to large amounts of data before the platform changes we announced in 2014, and we will audit any app where we identify suspicious activity. If we identify misuses of

data, we'll take immediate action, including banning the app from our platform and pursuing legal action if appropriate.

- *Tell people about data misuse.* We will tell people about apps that have misused their data. This includes building a way for people to know if their data might have been accessed via the app. Moving forward, if we remove an app for misusing data, we will tell everyone who used it.
- *Turn off access for unused apps.* If someone has not used an app within the last three months, we will turn off the app's access to their data.
- *Restrict Facebook Login data.* We are changing Login, so that the only data that an app can request without app review will include name, profile photo, and e-mail address. Requesting any other data will require approval from Facebook. We will also no longer allow apps to ask for access to information like religious or political views, relationship status and details, custom friends lists, education and work history, fitness activity, book reading and music listening activity, news reading, video watch activity, and games activity. We will encourage people to manage the apps they use. We already show people what apps their accounts are connected to and allow them to control what data they've permitted those apps to use. But we're making it easier for people to see what apps they use and the information they have shared with those apps.
- *Reward people who find vulnerabilities.* We launched the Data Abuse Bounty program so that people can report to us any misuses of data by app developers.
- *Update our policies.* We have updated our terms and Data Policy to explain how we use data and how data is shared with app developers.

Question 7. Will your team re-architect the Facebook platform software architecture to ensure that 3rd party applications do not have the ability to store and share data?

Answer. In April 2014, we announced that we would more tightly restrict our platform APIs to prevent abuse. At that time we made clear that existing apps would have a year to transition—at which point they would be forced (1) to migrate to the more restricted API and (2) be subject to Facebook's new review and approval protocols. A small number of developers asked for and were granted short-term extensions beyond the one-year transition period, the longest of which lasted several months. These extensions ended several years ago. A transition period of this kind is standard when platforms implement significant changes to their technology base and was necessary here to avoid disrupting the experience of millions of people. New apps that launched after April 30, 2014 were required to use our more restrictive platform APIs. We required apps seeking additional categories of data to undergo proactive review by our internal teams. We rejected more than half of the apps seeking these permissions, including the second version of Kogan's app.

We review apps to ensure that the requested permissions clearly improve the user experience and that the data obtained is tied to an experience within the app. We conduct a variety of manual and automated checks of applications on the platform for Policy compliance, as well as random sampling. When we find evidence of or receive allegations of violations, we investigate and, where appropriate, employ a number of measures, including restricting applications from our platform, preventing developers from building on our platform in the future, and taking legal action where appropriate.

Recently, we announced a number of additional steps we're taking to address concerns raised by Kogan's app.

- *Review our platform.* We will investigate all apps that had access to large amounts of data before the platform changes we announced in 2014, and we will audit any app where we identify suspicious activity. If we identify misuses of data, we'll take immediate action, including banning the app from our platform and pursuing legal action if appropriate.
- *Tell people about data misuse.* We will tell people about apps that have misused their data. This includes building a way for people to know if their data might have been accessed via the app. Moving forward, if we remove an app for misusing data, we will tell everyone who used it.
- *Reward people who find vulnerabilities.* We launched the Data Abuse Bounty program so that people can report to us any misuses of data by app developers.
- *Update our policies.* We have updated our terms and Data Policy to explain how we use data and how data is shared with app developers.

We are investing so much in security that our costs will increase significantly. But we want to be clear about what our priority is: protecting our community is more important than maximizing our profits.

As our CEO Mark Zuckerberg has said, when you are building something unprecedented like Facebook, there are going to be mistakes. What people should hold us accountable for is learning from the mistakes and continually doing better—and, at the end of the day, making sure that we're building things that people like and that make their lives better.

Question 8. How will you prevent another developer like Kogan from creating a viral app for the expressed purpose of gathering data and downloading, storing, and sharing that data?

See Response to Question 7.

Question 9. How do you know that there are no other copies of the data that Kogan acquired from Facebook?

Answer. Facebook obtained written certifications from Kogan, GSR, and other third parties (including Cambridge Analytica and SCL) declaring that all data they had obtained, and any derivatives, was accounted for and destroyed. Based on recent allegations, we have reopened our investigation into the veracity of these certifications and have hired a forensic auditor to conduct a forensic audit of Cambridge Analytica's systems. We are currently paused on the audit at the request of the UK Information Commissioner's Office request, which is conducting a regulatory investigation into Cambridge Analytica (based in the UK), and we hope to move forward with that audit soon.

We have suspended SCL/Cambridge Analytica from purchasing advertising on Facebook.

Question 10. A March 2018 online article in *Quartz* reported that Facebook employees and Cambridge Analytica employees were both working in the Trump Campaign San Antonio headquarters.[1] How will you ensure that your advertising salespeople are not engaging with entities previously identified for violating your terms of service?

Answer. No one from Facebook was assigned full-time to the Trump campaign, or full-time to the Clinton campaign. We offered identical support to both the Trump and Clinton campaigns, and had teams assigned to both. Everyone had access to the same tools, which are the same tools that every campaign is offered. We continuously work to ensure that we comply with all applicable laws and policies. While our investigation is ongoing, our review indicates that Facebook employees did not identify any issues involving the improper use of Facebook data in the course of their interactions with Cambridge Analytica during the 2016 U.S. Presidential campaign.

Question 11. In a recent press conference,[2] you state that you are fully confident you are making progress against foreign actor manipulating the Facebook platform. Will you provide Congress and the American people auditable periodic reports about the progress you and your team are making on fighting disinformation on your platform?

Answer. We have worked to notify people about this issue, broadly, through our white paper in April 2017, Information Operations on Facebook, and our disclosure about the IRA last fall. We have also been publishing updates on these issues in our Newsroom.

Question 12. Third Party Applications: How many times has Facebook enforced your terms of services against 3rd party application for misuse of data?

Answer. We use a variety of tools to enforce Facebook policies against violating parties, including developers. We review tens of thousands of apps per year and regularly disapprove noncompliant apps as part of our proactive review process. We also use tools like cease and desist letters, account suspensions, letter agreements, and civil litigation. For example, since 2006, Facebook has sent over 1,150 cease-and-desist letters to over 1,600 targets. In 2017, we took action against about 370,000 apps, ranging from imposing certain restrictions to removal of the app from the platform. Moreover, we have required parties who have procured our data without authorization to delete that data. We have invested significant resources in these efforts. Facebook is presently investigating apps that had access to large

---

[1] Kozlowska, Hanna. 20 March 2018. Facebook and Cambridge Analytica worked side by side at a Trump campaign office in San Antonio. *https://qz.com/1233579/facebook-and-cambridge-analytica-worked-side-by-side-at-a-trumpcampaign-office-in-san-antonio/*.

[2] Facebook. 4 April 2018. "Hard Questions: Q&A with Mark Zuckerberg on Protecting People's Information". *https://newsroom.fb.com/news/2018/04/hard-questions-protecting-peoples-information/*.

amounts of information before we changed our platform policies in 2014 to significantly reduce the data apps could access. To date around 200 apps (from a handful of developers: Kogan, AIQ, Cube You, the Cambridge Psychometrics Center, and myPersonality) have been suspended—pending a thorough investigation into whether they did in fact misuse any data.

Question 13. It's clear that, over the course of the Facebook platform program, enforcement of the Platform Policy has been reactive rather than proactive. Of all the 3rd party applications, how many such applications have been reviewed in the past 8 years? How many 3rd party applications have been removed from the platform due to violations of the terms of service?

Answer. See Response Question 12.

Question 14. According to your Platform Policy, if you exceed 5 million monthly active users or 100M API calls per day, developers may be subject to additional terms. What are the additional terms? How many 3rd party applications are currently subject to additional terms?

Answer. In circumstances where developers make a high volume of API calls, Facebook may impose additional terms, which are generally negotiated and vary depending on which APIs are at issue.

In addition, Facebook has a set of APIs that enable certain partners, primarily operating systems and device manufacturers, to provide people with Facebook-like experiences (*e.g.,* Facebook apps, news feed notifications, address book syncs) in their products. We developed these APIs, which are commonly known as "device-integrated APIs," in the early days of mobile when the demand for Facebook outpaced our ability to build versions of our product that worked on every phone or operating system. Several dozen companies still used them at the start of the year, including Amazon, Apple, Blackberry, HTC, Microsoft, Huawei, Lenovo and Samsung, among others. On April 23, 2018, we announced that we would wind down these APIs. So far over 30 of these partnerships have been ended, including with Huawei.

These device-integrated APIs are different from the platform APIs that were used by Alexandr Kogan, which were the focus of the hearing and went to the heart of the Cambridge Analytica matter. Third party developers using our platform APIs built new, social experiences incorporating information that Facebook users brought with them; by contrast, the very point of our device-integrated APIs was to enable other companies to create Facebook functionality, primarily for devices and operating systems. The experiences that partners built using our device-integrated APIs were reviewed and approved by Facebook, and partners could not integrate the user's Facebook features without the user's permission.

Question 15. For the Platform Policy for Messenger, how do you ensure that malicious actors are not using bots using the Messenger API to spread disinformation to users at a mass scale?

Answer. Businesses large and small are using bots for Messenger to connect with their customers in a way that is convenient, functional, and enables them to connect with customers at scale. We give people control of their experience. We offer a set of tools that allow a person to block or mute a bot or business at any time and people can also report bots where the Facebook Community Operations team will review and take action if appropriate. Finally, a few months ago we announced that bot developers are now required to have business verification for apps/bots that need access to specialized APIs as a result of our ongoing efforts to ensure integrity across our platforms.

Question 16. Facebook—Suite of Application—Onavo VPN: Do know whether customers who download the virtual private network, or VPN, of Facebook's subsidiary Onavo's understand that any activity occurring on their mobile device is being collected and stored by Facebook? Doesn't this practice violate the privacy consumers expect of a VPN?

Answer. When people first install the iOS version of the Onavo Protect app, we explain that Onavo uses a VPN that "helps keep you and your data safe by understanding when you visit potentially malicious or harmful websites and giving you a warning." In addition, the first screen that a person sees when installing the app explains, under a heading that reads "Data Analysis":

> "When you use our VPN, we collect the info that is sent to, and received from, your mobile device. This includes information about: your device and its location, apps installed on your device and how you use those apps, the websites you visit, and the amount of data use.
>
> This helps us improve and operate the Onavo service by analyzing your use of websites, apps and data. Because we're a part of Facebook, we also use this info

to improve Facebook products and services, gain insights into the products and services people value, and build better experiences."

People must tap a button marked "Accept & Continue" after seeing this information in a full-screen interstitial before they can use the app.

The Android version of the Onavo Protect app offers data management features (*e.g.,* the ability to block apps from using background data) that do not require users to enable the app's VPN.

For both versions of the app, we communicate repeatedly and up front—in the App Store description, in Onavo's Privacy Policy, and in-line at the time the user first opens the app after downloading it—that Onavo is part of Facebook and what that means for how Onavo Protect handles data in other ways.

More broadly, websites and apps have used market research services for years. We use Onavo, App Annie, comScore, and publicly available tools to help us understand the market and improve all our services. When people download Onavo to manage their data usage and help secure their connection, we are clear about the information we collect and how it is used. Like other VPNs, when the Onavo VPN is enabled, Onavo Protect helps create a secure connection, including when people are on public Wi-Fi. As part of this process, Onavo receives their mobile data traffic. This helps us improve and operate the Onavo service. Because we're part of Facebook, we also use this information to improve Facebook products and services. We let people know about this activity, and other ways that Onavo uses, analyzes, and shares data (for example, the apps installed on users' devices) in the App Store descriptions, and when they first open the app after downloading it.

Facebook does not use Onavo data for Facebook product uses, nor does it append any Onavo data or data about individuals' app usage to Facebook accounts.

Question 17. According to this *Wall Street Journal* article, Facebook uses data collected from the Onavo suite of applications to monitor potentially competitive application.[3] Since the acquisition in 2013, how specifically has Facebook used information from Onavo to inform acquisitions as well as product development?

Answer. See Response to Question 16.

Question 18. Terms of Service: Has Facebook ever disclosed to its users which "third parties partners" have access to user information? If no, will you publish this list so that users know which outside parties have access to their information?

Answer. Facebook allows people to view, manage, and remove the apps that they have logged into with Facebook through the App Dashboard. We recently prompted everyone to review their App Dashboard as a part of a Privacy Checkup, and we also provided an educational notice on Facebook to encourage people to review their settings. More information about how users can manage their app settings is available at *https://www.facebook.com/help/218345114850283?helpref=about_content.*

The categories of information that an app can access is clearly disclosed before the user consents to use an app on Facebook platform. Users can view and edit the categories of information that apps they have used have access to through the App Dashboard.

Question 19. User Tracking: Does Facebook can "track a user's Internet browsing activity, even after that user has logged off of the Facebook platform"? If yes, how Facebook discloses that kind of tracking to its users? And can users opt-out of this kind of tracking?

Answer. When people visit apps or websites that feature our technologies—like the Facebook Like or Comment button—our servers automatically log (i) standard browser or app records of the fact that a particular device or user visited the website or app (this connection to Facebook's servers occurs automatically when a person visits a website or app that contains our technologies, such as a Like button, and is an inherent function of Internet design); and (ii) any additional information the publisher of the app or website chooses to share with Facebook about the person's activities on that site (such as the fact that a purchase was made on the site). This is a standard feature of the Internet, and most websites and apps share this same information with multiple different third-parties whenever people visit their website or app. For example, the Senate Commerce Committee's website shares information with Google and its affiliate DoubleClick and with the analytics company Webtrends. This means that, when a person visits the Committee's website, it sends browser information about their visit to each one of those third parties. More information about how this works is available at *https://newsroom.fb.com/news/2018/04/data-off-facebook/*.

---

[3] Seetharaman, Deepa and Morris, Betsy. "Facebook's Onavo Gives Social-Media Firm Inside Peek at Rivals' Users." 13 August 2017. Wall Street Journal.

When the person visiting a website featuring Facebook's tools is not a registered Facebook user, Facebook does not have information identifying that individual, and it does not create profiles for this individual.

We use the browser and app logs that apps and websites send to us—described above—in the following ways for non-Facebook users. First, these logs are critical to protecting the security of Facebook and to detecting or preventing fake account access. For example, if a browser has visited hundreds of sites in the last five minutes, that's a sign the device might be a bot, which would be an important signal of a potentially inauthentic account if that browser then attempted to register for an account. Second, we aggregate those logs to provide summaries and insights to websites and apps about how many people visit or use their product, or use specific features like our Like button—but without providing any information about a specific person. We do not create profiles for non-Facebook users, nor do we use browser and app logs for non-Facebook users to show targeted ads from our advertisers to them or otherwise seek to personalize the content they see. However, we may take the opportunity to show a general ad that is unrelated to the attributes of the person or an ad encouraging the non-user to sign up for Facebook.

When the individual is a Facebook user, we are also able to use this information to personalize their experiences on Facebook, whether or not they are logged out, but we will not target ads to users relying on this information unless the user allows this in their privacy settings. We do not sell or share this information with third-parties.

Question 20. How many Facebook "Like" buttons there are on non-Facebook web pages?

Answer. Facebook does not publish tracking software. When people visit apps or websites that feature our technologies—like the Facebook Like or Comment button—our servers automatically log (i) standard browser or app records of the fact that a particular device or user visited the website or app (this connection to Facebook's servers occurs automatically when a person visits a website or app that contains our technologies, such as a Like button, and is an inherent function of Internet design); and (ii) any additional information the publisher of the app or website chooses to share with Facebook about the person's activities on that site (such as the fact that a purchase was made on the site).

This is a standard feature of the Internet, and most websites and apps share this same information with multiple different third-parties whenever people visit their website or app. For example, the Senate Commerce Committee's website shares information with Google and its affiliate DoubleClick and with the analytics company Webtrends. This means that, when a person visits the Committee's website, it sends browser information about their visit to each one of those third parties. More information about how this works is available at *https://newsroom.fb.com/news/2018/04/data-off-facebook/*.

During the week prior to April 16, 2018, on sites that use Facebook services: the Like button appeared on 8.4M websites, the Share button on 931K websites covering 275M webpages, and there were 2.2M Facebook pixels installed on websites.

Question 21. How many Facebook "Share" buttons there are on non-Facebook web pages?

Answer. See Response to Question 20.

Question 22. How many non-Facebook websites have Facebook pixel code?

Answer. See Response to Question 20.

Question 23. While users can download their user generated data using the "Download Your Information" tool, how can users download data that Facebook has inferred about them?

Answer. Our Download Your Information or "DYI" tool is Facebook's data portability tool and was launched many years ago to let people access and download many types of information that we maintain about them. The data in DYI and in our Ads Preferences tool contain each of the interest categories that are used to show people ads, along with information about the advertisers are currently running ads based on their use of an advertiser's website or app. People also can choose not to see ads from those advertisers. We recently announced expansions to Download Your Information, which, among other things, will make it easier for people to see their data, delete it, and easily download and export it. More information is available at *https://newsroom.fb.com/news/2018/04/new-privacy-protections/*.

Responding to feedback that we should do more to provide information about websites and apps that send us information when people use them, we also announced plans to build Clear History. This new feature will enable users to see the websites and apps that send us information when they use them, delete this infor-

mation from their account, and turn off Facebook's ability to store it associated with their account going forward.

We have also introduced Access Your Information. This feature provides a new way for people to access and manage their information. Users can go here to delete anything from their timeline or profile that they no longer want on Facebook. They can also see their ad interests, as well as information about ads they've clicked on and advertisers who have provided us with information about them that influence the ads they see. From here, they can go to their ad settings to manage how this data is used to show them ads.

Question 24. How many websites have Facebook-tracking software on them? What percentage of all Internet sites have Facebook-tracking software?

Answer. See Response to Question 20.

Question 25. According to a Gizmodo report,[4] Facebook collects data on people using Shadow Profiles. Do you collect data on people who are not Facebook users? Please describe the process for non-Facebook users can employ to delete any data collected about them by the company.

Answer. Yes. If a person doesn't have a Facebook account but believes Facebook may have information about them, they can contact us to request a copy of your information. A contact form is available at *https://www.facebook.com/help/contact/180237885820953.* However, Facebook does not create profiles about or track web or app browser behavior of non-users.

When people visit apps or websites that feature our technologies—like the Facebook Like or Comment button—our servers automatically log (i) standard browser or app records of the fact that a particular device or user visited the website or app (this connection to Facebook's servers occurs automatically when a person visits a website or app that contains our technologies, such as a Like button, and is an inherent function of Internet design); and (ii) any additional information the publisher of the app or website chooses to share with Facebook about the person's activities on that site (such as the fact that a purchase was made on the site). This is a standard feature of the Internet, and most websites and apps share this same information with multiple different third-parties whenever people visit their website or app. For example, the Senate Commerce Committee's website shares information with Google and its affiliate DoubleClick and with the analytics company Webtrends. This means that, when a person visits the Committee's website, it sends browser information about their visit to each one of those third parties. More information about how this works is available at *https://newsroom.fb.com/news/2018/04/data-off-facebook/*.

When the person visiting a website featuring Facebook's tools is not a registered Facebook user, Facebook does not have information identifying that individual, and it does not create profiles for this individual.

We use the browser and app logs that apps and websites send to us—described above—in the following ways for non-Facebook users. First, these logs are critical to protecting the security of Facebook and to detecting or preventing fake account access. For example, if a browser has visited hundreds of sites in the last five minutes, that's a sign the device might be a bot, which would be an important signal of a potentially inauthentic account if that browser then attempted to register for an account. Second, we aggregate those logs to provide summaries and insights to websites and apps about how many people visit or use their product, or use specific features like our Like button—but without providing any information about a specific person.

We do not create profiles for non-Facebook users, nor do we use browser and app logs for non-Facebook users to show targeted ads from our advertisers to them or otherwise seek to personalize the content they see. However, we may take the opportunity to show a general ad that is unrelated to the attributes of the person or an ad encouraging the non-user to sign up for Facebook.

Question 26. Do you support a kids' privacy bill of rights where opt-in is the standard?

Answer. Facebook is generally not opposed to regulation but wants to ensure it is the right regulation. The issues facing the industry are complex, multi-faceted, and affect an important part of peoples' lives. As such, Facebook is absolutely committed to working with regulators, like Congress, to craft the right regulations. Facebook would be happy to review any proposed legislation and provide comments.

---

[4] Hill, Kasmir. 07 November 2017. How Facebook Figures Out Everyone You've Met. Gizmodo. *https://gizmodo.com/how-facebook-figures-out-everyone-youve-ever-met-1819822691?IR=T.*

RESPONSE TO WRITTEN QUESTIONS SUBMITTED BY HON. GARY PETERS TO MARK ZUCKERBERG

Question 1. A major challenge artificial intelligence (AI) and machine learning developers need to address is the ability to ensure prolonged safety, security, and fairness of the systems. This is especially true of systems designed to work in complex environments that may be difficult to replicate in training and testing, or systems that are designed for significant learning after deployment. One approach to address this challenge is to implement standards or principles guiding the development of AI systems. However, you referenced AI more than 30 times in your testimony on Capitol Hill, and many of those references were in different contexts. This seems to imply Facebook has assumed a broad or vague definition of AI. I fear that a vague definition will make it difficult to implement clear, unambiguous standards or principles to guide the fair, safe, and secure application of AI and algorithms.

- What how does Facebook define AI?
- How is Facebook currently working to build trust in its usage of AI? Specifically, has your company developed a set of principles to guide your development and use of AI systems? If so, what are they? Please also provide details on how these principles are being implemented.
- How will these principles improve the transparency of decision-making AI systems?
- How will these principles prevent a system designed to learn after deployment from developing unacceptable behavior over time?

Answer. We are focused on both the technical and the ethical aspects of artificial intelligence. We believe these two should go hand-in-hand together in order to fulfill our commitment to being fair, transparent and accountable in our development and use of AI. Facebook has AI teams working on developing the philosophical, as well as technical, foundations for this work. Facebook is also one of the co-founders and members of the Partnership on AI (PAI), a collaborative and multi-stakeholder organization established to study and formulate best practices on AI technologies, to advance the public's understanding of AI, and to serve as an open platform for discussion and engagement about AI and its influences on people and society. The thematic pillars that structure the work we're doing in the scope of the PAI—safety, fairness, transparency and accountability—are the principles that we believe industry should follow and promote when building and deploying AI systems. The PAI's Fair, Transparent and Accountable AI Working Group is also working alongside industry, academia, and civil society to develop best practices around the development and fielding of fair, explainable, and accountable AI systems.

We believe that over the long term, building AI tools is the scalable way to identify and root out most content that violates our policies. We are making substantial investments in building and improving these tools. We already use artificial intelligence to help us identify threats of real world harm from terrorists and others. For example, the use of AI and other automation to stop the spread of terrorist content is showing promise. Today, 99 percent of the ISIS and Al Qaeda related terror content we remove from Facebook is content we detect before anyone in our community has flagged it to us, and in some cases, before it goes live on the site. We do this primarily through the use of automated systems like photo and video matching and text-based machine learning. We also use AI to help find child exploitation images, hate speech, discriminatory ads, and other prohibited content.

Question 2. Mr. Zuckerberg, you said recently that Facebook is more like a government than a traditional company. Facebook is a community of over 2 billion people from every country in the world. You have also said you hope to grow the number of Facebook employees working on security of the user community to 20,000 by the end of the year. A city like Flint, Michigan has a population of 100,000 and roughly 100 uniformed police officers. Your company is aiming to have one cop on the beat for every 100,000 of its 2 billion users.

- Is this going to be adequate to prevent another misuse of consumer data like we saw with Cambridge Analytica?

Answer. We are doubling the size of our security and content review teams (from 10,000 to 20,000) over the course of this year. We currently have approximately 15,000 people working on these teams.

Question 3. How are you making the efforts of these employees transparent and accountable to your users?

Answer. We are taking significant steps to increase our transparency. For example, we have published the internal guidelines we use to enforce our Community

Standards here: *https://newsroom.fb.com/news/2018/04/comprehensive-community-standards/*. We decided to publish these internal guidelines for two reasons. First, the guidelines will help people understand where we draw the line on nuanced issues. Second, providing these details makes it easier for everyone, including experts in different fields, to give us feedback so that we can improve the guidelines—and the decisions we make—over time.

We also recently publicized data around enforcement of our Community Standards in a Community Standards Enforcement Report (*https://transparency.facebook.com/community-standards-enforcement*). The report details our enforcement efforts between October 2017 to March 2018, and it covers six areas: graphic violence, adult nudity and sexual activity, terrorist propaganda, hate speech, spam, and fake accounts. The numbers show you:

- How much content people saw that violates our standards;
- How much content we removed; and
- How much content we detected proactively using our technology—before people who use Facebook reported it.

The data we published is the same information we use to measure our progress internally.

We believe this increased transparency will lead to increased accountability and responsibility over time.

Question 4. Facebook has made some changes in light of the 2016 U.S. Presidential election and the fact that your platform allowed for the proliferation of fake news. You've since developed tools that try to tamp down on this activity—pulling down fake accounts and destroying bots.

- You have described the content on your platform during elections held since 2016, both foreign and domestic, as "cleaner"—but what metrics are you using to evaluate the real effectiveness of the changes you have made?
- Once you have a true understanding of the impact these tools have—how can you communicate the changes to users so they can be confident that what they are viewing is real and not there for the purpose of manipulating them?
- Consumers are skeptical of the content on your platform, how can you gain back their trust?

Answer. We are working hard to regain the trust of our community.

Success would consist of minimizing or eliminating abuse of our platform and keeping our community safe. We have a number of specific goals that we will use to measure our progress in these efforts. First, we are increasing the number of people working on safety and security at Facebook, to 20,000. We have significantly expanded the number of people who work specifically on election integrity, including people who investigate this specific kind of abuse by foreign actors. Those specialists find and remove more of these actors. Second, we work to improve threat intelligence sharing across our industry, including, we hope, by having other companies join us in formalizing these efforts. This is a fight against sophisticated actors, and our entire industry needs to work together to respond quickly and effectively. Third, we are bringing greater transparency to election ads on Facebook by requiring more disclosure from people who want to run election ads about who is paying for the ads and by making it possible to see all of the ads that an advertiser is running, regardless of the targeting. We believe that these efforts will help to educate our community and to arm users, media, civil society, and the government with information that will make it easier to identify more sophisticated abuse to us and to law enforcement.

We have gotten increasingly better at finding and disabling fake accounts. We're now at the point that we block millions of fake accounts each day at the point of creation before they do any harm.

We are taking steps to help users assess the content they see on Facebook. For example, for ads with political content, we've created an archive that will hold ads with political content for seven years—including for information about ad impressions and spend, as well as demographic data such as age, gender and location. People in Canada and Ireland can already see all the ads that a Page is running on Facebook—and we're launching this globally in June. Further, advertisers will now need to confirm their ID and location before being able to run any ads with political content in the U.S. All ads with political content will also clearly state who paid for them. We also want to empower people to decide for themselves what to read, trust, and share. We promote news literacy and work to inform people with more context. For example, if third-party fact-checkers write articles about a news story, we show them immediately below the story in the Related Articles unit. We also

notify people and Page Admins if they try to share a story, or have shared one in the past, that's been determined to be false.

Question 5. How did Facebook, prior to the 2016 U.S. Presidential election, identify and evaluate fake or troll accounts, and how have your processes changed since then?

- What steps are taken once Facebook has identified fake or troll accounts and, specifically, how much of your response is consumer-facing? Will a user ever truly know the extent to which they were influenced by a fake account?

Answer. We continue to make improvements to our efforts to more effectively detect and deactivate fake accounts to help reduce the spread of spam, false news, and misinformation. We continually update our technical systems to identify, checkpoint, and remove inauthentic accounts, and we block millions of attempts to register fake accounts every day. These systems examine thousands of detailed account attributes and prioritize signals that are more difficult for bad actors to disguise, such as their connections to others on our platform. As with all security threats, we have been incorporating new insights into our models for detecting fake accounts, including information specific to election issues.

Question 6. Is it true that Facebook does not authenticate the administrators of group and organization pages in the same manner it authenticates individual accounts? Will you take a different approach going forward?

Answer. We have announced that people who manage Pages with large numbers of followers will need to be verified. Those who manage large Pages that do not clear the process will no longer be able to post. This will make it much harder for people to administer a Page using a fake account, which is strictly against our policies. We will also show users additional context about Pages to effectively assess their content. For example, a user can see whether a Page has changed its name.

Question 7. Current sector-specific privacy laws and state privacy laws, as well as currently proposed Federal legislation that address data privacy and security, often narrowly define personal information to include identifiers like a person's name, social security number, and bank information. But definitions of personal information currently do not cover information like social media "likes" and certain choices and activities online that bad actors have at worst used to manipulate voters and at best used to deliver targeted advertisements.

- What do you think Cambridge Analytica has taught us about what should be considered personal information?
- Should definitions of personal information be updated to include an individual's activities like search activity and social media "likes"?

Answer. Facebook is generally not opposed to regulation but wants to ensure it is the right regulation. The issues facing the industry are complex, multi-faceted, and affect an important part of peoples' lives. As such, Facebook is absolutely committed to working with regulators, like Congress, to craft the right regulations. Facebook would be happy to review any proposed legislation and provide comments.

Question 8. Who do you consider to be Facebook's customers (*i.e.,* what stakeholders directly provide Facebook with revenue)? To the extent that the customers are not the end users of the platform, how will Facebook reconcile the privacy expectations and interests of both sets of stakeholders?

Answer. In the words of Facebook CEO and Founder Mark Zuckerberg, "Facebook is an idealistic and optimistic company. For most of our existence, we focused on all the good that connecting people can bring. As Facebook has grown, people everywhere have gotten a powerful new tool to stay connected to the people they love, make their voices heard, and build communities and businesses." Our product is social media—the ability to connect users with the people that matter to them, wherever they are in the world. It's the same with a free search engine, website or newspaper. The core product is reading the news or finding information—and the ads exist to fund that experience. Our priority is protecting our community, and that is more important than maximizing our profits.

Question 9. Does Facebook intend to provide its users with a comprehensive listing of all apps and services that have accessed their Facebook data? In such a listing, would Facebook include information about which data points were accessed, when they were accessed, and how they were accessed?

Answer. Facebook allows people to view, manage, and remove the apps that they have logged into with Facebook through the App Dashboard. We recently prompted everyone to review their App Dashboard as a part of a Privacy Checkup, and we also provided an educational notice on Facebook to encourage people to review their

settings. More information about how users can manage their app settings is available at *https://www.facebook.com/help/218345114850283?helpref=aboutcontent.*

The categories of information that an app can access is clearly disclosed before the user consents to use an app on Facebook platform. Users can view and edit the categories of information that apps they have used have access to through the App Dashboard.

Question 10. What mechanisms does Facebook have in place to monitor third parties who have access to user data once the data is delivered? If a user deletes their data on Facebook, how does Facebook ensure that third parties with access to their data have also deleted it?

Answer. We use a variety of tools to enforce Facebook policies against violating parties, including developers. We review tens of thousands of apps per year. With the exception of Account Information (name, e-mail, gender, birthday, current city, and profile picture URL), apps may maintain user data obtained from us only for as long as necessary for their business purpose and must delete the information if they stop using the Facebook Platform. Further, developers are required to keep the data maintained on their systems up to date.

Question 11. What mechanisms—beyond self-reporting—are currently in place, or will be in place in the future, to enable independent academic and journalistic validation of Facebook's current and future claims that the platform has removed bad actors who have abused or compromised user data and privacy?

Answer. *App Review.* We have large teams of internal and external experts working hard to investigate these apps as quickly as possible. To date, thousands of apps have been investigated and around 200 (from a handful of developers) have been suspended—pending a thorough investigation into whether they did in fact misuse any data.

The App Review process introduced in 2014 requires developers who create an app that asks for more than certain basic user information from installers to justify the data they are looking to collect and how they are going to use it. Facebook then reviews whether the developer has a legitimate need for the data in light of how the app functions. Only if it is approved following such review can the app ask for users' permission to get their data. Facebook has rejected more than half of the apps submitted for App Review between April 2014 and April 2018.

New Developer Requirements. We are in the process of investigating every app that had access to a large amount of information before we changed our Platform in 2014. If we find suspicious activity, we will take immediate steps to investigate (including a full forensic audit) or take enforcement actions against the app. If we determine that there has been improper use of data, we will ban those developers and notify everyone affected. Facebook is launching the Data Abuse Bounty to reward people who report any misuse of data by app developers. The Data Abuse Bounty, inspired by the existing bug bounty program that we use to uncover and address security issues, will help us identify violations of our policies.

Further, Facebook's Platform Policy makes clear to app developers the relevant requirements regarding users' privacy that apply to apps operating on the Platform, including the requirements to give users choice and control, and to respect user privacy. Application developers explicitly agree to Facebook's Statement of Rights and Responsibilities and Platform Policy when they set up their Facebook accounts. The Platform Policy imposes a variety of obligations on app developers regarding the features, functionality, data collection and usage, and content for apps on the Platform, as well as Facebook's right to take enforcement action if an application violates the Platform Policy.

Clear History. We have also worked with regulators, legislators, and privacy experts on updates that make data settings and tools easier to find. For example, we recently announced plans to build Clear History. This feature will enable users to see the websites and apps that send us information when they use them, delete this information from their accounts, and turn off our ability to store it associated with their accounts going forward. When developing tools such as Clear History, we will work with privacy advocates, academics, policymakers, and regulators to get their input on our approach, including how we plan to remove identifying information and the rare cases where we need information for security purposes. We've already started a series of roundtables in cities around the world, and heard specific demands for controls like these at a session we held at our headquarters two weeks ago. We're looking forward to doing more.

Measuring Misinformation Through Academic Commission. In April, Facebook also announced a new initiative to help provide independent research about the role of social media in elections, as well as democracy more generally. In the coming weeks, the commission will lead a request for proposals to measure the volume and

effects of misinformation on Facebook. They will then manage a peer review process to select which scholars will receive funding for their research, and access to privacy-protected data sets from Facebook. This will help keep us accountable and track our progress over time.

Elections. We know that outside experts, researchers, and academics can also help by analyzing political advertising on Facebook. It's why we're working closely with our newly-formed Election Commission and other stakeholders to launch an API for the archive of ads with political content. We also recognize that news coverage of elections and important issues is distinct from advocacy or electoral ads, even if those news stories receive paid distribution on Facebook. We're working closely with news partners and are committed to updating the archive to help differentiate between news and non-news content.

Question 12. Well, you bring up the principles because, as you are well aware, AI systems, especially in very complex environments when you have machine learning, it is sometimes very difficult to understand, as you mentioned, exactly how those decisions were arrived at. There are examples of how decisions are made on a discriminatory basis and that they can compound if you are not very careful about how that occurs. And so is your company—you mentioned principles. Is your company developing a set of principles that are going to guide that development? And would you provide details to us as to what those principles are and how they will help deal with this issue?

Answer. We are focused on both the technical and the ethical aspects of artificial intelligence. We believe these two should go hand-in-hand together in order to fulfill our commitment to being fair, transparent, and accountable in our development and use of AI. Facebook has AI teams working on developing the philosophical, as well as technical, foundations for this work. Facebook is also one of the co-founders and members of the Partnership on AI (PAI), a collaborative and multi-stakeholder organization established to study and formulate best practices on AI technologies, to advance the public's understanding of AI, and to serve as an open platform for discussion and engagement about AI and its influences on people and society. The thematic pillars that structure the work we're doing in the scope of the PAI—safety, fairness, transparency, and accountability—are the principles that we believe industry should follow and promote when building and deploying AI systems. The PAI's Fair, Transparent and Accountable AI Working Group is also working alongside industry, academia, and civil society to develop best practices around the development and fielding of fair, explainable, and accountable AI systems.

Response to Written Questions Submitted by Hon. Tammy Baldwin to Mark Zuckerberg

Question 1. Do you know whether Aleksandr Kogan sold any of the data he collected to anyone other than Cambridge Analytica?

Answer. Kogan represented to us that he provided data to SCL, Eunoia Technologies (a company founded by Christopher Wylie), and a researcher at the Toronto Laboratory for Social Neuroscience at the University of Toronto. He represented to Facebook that he only received payment from SCL/Cambridge Analytica.

Question 2. How much do you know or have you tried to find out how Cambridge Analytica used the data while they had it before you believed they deleted it?

Answer. On December 11, 2015, *The Guardian* published an article reporting that Kogan and his company, GSR, may have passed information his app had obtained from Facebook users to SCL Elections Ltd. (SCL)/Cambridge Analytica. By doing so, Kogan and his company violated Facebook's Platform Policies, which explicitly prohibited selling or licensing user data accessed from Facebook and from sharing any user data accessed from Facebook with any ad network, data broker or other advertising or monetization-related service. For this reason, Facebook immediately banned his app from our platform and launched an investigation into these allegations. Kogan signed a certification declaring that he had deleted all data that he obtained through his app and obtained certifications of deletion from others he had shared data with, including Cambridge Analytica. In March 2018, new allegations surfaced that Cambridge Analytica may not have deleted data as it had represented. Our investigation of these matters is ongoing.

Question 3. I find some encouragement in the steps you have outlined today to provide greater transparency regarding political ads. I want to get further information on how you can be confident that you have excluded entities based outside of the United States.

Answer. Pursuant to the new transparency measures Facebook is launching, all advertisers who want to run ads with political content targeted at the U.S. will have to confirm their identity and location by providing either a U.S. driver's license or passport, last four digits of their social security number, and a residential mailing address. In addition, people who manage Pages with large numbers of followers will need to be verified. Those who manage large Pages that do not clear the process will no longer be able to post.

RESPONSE TO WRITTEN QUESTIONS SUBMITTED BY HON. TAMMY DUCKWORTH TO MARK ZUCKERBERG

Question 1. According to the *New York Times* and other media outlets, fair housing advocates recently filed a lawsuit in Federal court arguing that "Facebook continues to discriminate against certain groups, including women, disabled veterans and single mothers, in the way that it allows advertisers to target the audience for their ads." Despite repeated announcements by Facebook suggesting that your company will remedy this disturbing practice, third-party organizations have tested your platform repeatedly to exclude certain minorities. Unfortunately, many of these tests of your platform were successful and this issue has been known to Facebook for several years.

Please explain in detail why Facebook provided housing advertisers with targeting options to exclude users based on "ethnic affinity" in clear violation of Federal law. Following third-party demonstrations of how a housing advertiser could unlawfully use Facebook to discriminate against certain protected classes of housing customers, please describe in detail the specific actions Facebook took to end the practice and make sure that Facebook's user tools actually reflect Facebook's written policies that claim to prohibit using Facebook's targeting options to discriminate. As Chairman and Chief Executive Officer, please describe how you personally responded to the public reports demonstrating that Facebook's targeting options had enabled unlawful discrimination in housing. Please provide any company documents, in hard copy or electronic form, addressing the implementation of Facebook advertising targeting options and any associated risk that such an option could result in violations of Federal legal prohibitions against discrimination in housing. If Facebook has no such documents, please provide a detailed justification as to why the company did not, or does not, have a compliance protocol or office dedicated to enforcing Fair Housing laws.

Answer. We want our advertising tools to help promote inclusion and diversity of all kinds. Discrimination has no place on Facebook, and we make this clear to advertisers in a number of ways. Everyone on Facebook must agree to our Terms when they sign up to use our service. In so doing, they agree not to engage in discriminatory conduct on Facebook. In addition, our Advertising Policies (available at *https://www.facebook.com/policies/ads/*) include an explicit and detailed anti-discrimination policy that prohibits discriminatory ads or the use of our audience selection tools for discriminatory purposes.

In late 2016, we began building machine learning tools (called "classifiers") that were intended to automatically identify, at the point of creation, advertisements offering housing, employment or credit opportunities (referred to here generally as "housing, employment and credit ads"). We built these classifiers so that when we identified one of these kinds of ads, we could: (1) prevent the use of our "multicultural affinity" targeting options in connection with the ad, and (2) for the use of any other kind of targeting, require that the advertiser certify compliance with our anti-discrimination policy and applicable anti-discrimination laws.

We trained the classifiers before we launched them, including by using search terms provided by your office in January 2017. After the classifiers launched in approximately February 2017, we anticipated that, through machine learning, they would become better over time at distinguishing ads offering housing, employment, or credit opportunities from other types of ads. We also expected that we would receive feedback about the performance of the tool that would enable us to detect problems and improve the classifiers over time.

In practice, the classifiers did not improve over time as much as we had anticipated. Rather, they became both over- and under-inclusive, identifying and requiring self-certification for hundreds of thousands of ads each day that may have had nothing to do with housing, employment, or credit offers, while missing ads that may have contained such offers.

There were two principal reasons for this failure. First, a key aspect of our ad-review process involves the random sampling of ads that are live on Facebook for the purpose of reassessing those ads' compliance with our Advertising Policies.

When we identify ads that should have been flagged as being in violation of our policies, we use that information to improve our review processes, including our machine learning classifiers. In hindsight, our training set was not sufficiently comprehensive and did not include an evolving set of housing, credit and employment ads that should have been flagged by our classifiers to better train our models. We also failed to fully account for the lack of feedback we would likely receive about the performance of these classifiers through other channels—feedback we typically rely on to alert us to performance issues. For example, advertisers whose ads should have been (but were not) identified through this process would have had no reason to report a problem.

We take these limitations very seriously, and we regret that they prevented us from providing the oversight we had hoped to provide. Since they were brought to our attention in November 2017, we have taken significant steps to remedy them. These steps include the following:

- We have integrated all of the classifiers and targeting prohibitions into the random sampling process we use to gather feedback about the performance of our ad review processes.
- We are adding more than 1,000 people to our global ads review teams over the next year to allow for more human review of the ads placed on our platform.
- We have built teams whose role it is to pressure test our policy-enforcement products to identify potential performance issues.

In addition to addressing the issues with housing, employment and credit classifiers to more accurately identify such ads, as of January 2018, we have implemented the following additional changes with regard to multicultural affinity targeting more generally:

- We disabled the use of multicultural affinity exclusion targeting for all ads; this prohibition is no longer limited to housing, employment and credit ads.
- We now require self-certification of compliance with our anti-discrimination policies and applicable anti-discrimination laws for any use of multicultural affinity targeting, regardless of the type of ad.
- We have undertaken a review of our ad-targeting tools generally, with an eye toward identifying the potential for the tools to be abused.
- As a result of that review, we disabled the use of other exclusion targeting categories that we determined, on their face, may have been misunderstood to identify a group of Facebook users based on race, color, national origin or ancestry.

Question 2. What is Facebook doing to protect Veterans, women and other minorities to ensure that advertisements on your platform do not discriminate against them in possible violation of Federal laws? Is Facebook aware of an investigation by the U.S. Department of Housing and Urban Development regarding these issues and is Facebook cooperating with an investigation? When were you alerted that an investigation(s) had begun? Do you believe that violators of Federal laws prohibiting discrimination, such as the protections contained in the Fair Housing Act, should be held accountable?

Answer. Discriminatory advertising has no place on Facebook's platform and Facebook removes such content as soon as it becomes aware of it. Facebook's policies prohibit advertisers from discriminating against people on personal attributes such as race, ethnicity, color, national origin, religion, age, sex, sexual orientation, gender identity, family status, disability, and medical or genetic conditions. Facebook educates advertisers on our anti-discrimination policy, and in some cases, requires the advertisers to certify compliance with Facebook's anti-discrimination policy and anti-discrimination laws.

Facebook also uses machine learning to help identify ads that offer housing, employment, or credit opportunities. When an advertiser attempts to show an ad that Facebook identifies as offering a housing, employment, or credit opportunity and includes Facebook's multicultural advertising segments, Facebook will disapprove the ad. Facebook also requires advertisers to certify that they are complying with Facebook's updated anti-discrimination policy and anti-discrimination laws when the advertiser attempts to show a housing, employment, or credit opportunity and uses any other audience segment on Facebook.

Facebook has been actively engaged with the U.S. Department of Housing and Urban Development (HUD) since at least the Fall of 2016. As part of the engagement, Facebook has focused on addressing the concern that advertisers may seek to engage in discriminatory advertising on Facebook's platform. In connection with

this engagement, Facebook has made numerous modifications and improvements to its ad policies, practices, and tools.

Question 3. I'm glad to hear that Facebook plans to extend the European Union's General Data Protection Regulations (GDPR) to U.S. users. By what date does Facebook plan on extending those protections to U.S. users? In doing so, is Facebook affirming that all data generated by a user is the property of that user and is subject to protections outlined in the General Data Protection Regulations, including rights to access, rectification, erasure, data portability, among others?

Answer. We confirm that we provide the same tools for access, rectification, erasure, data portability and others to people in the U.S. (and globally) that we provide in the European Union, and many of those tools (like our Download Your Information tool, Ad Preferences tool, and Activity Log) have been available globally for many years. We have recently begun providing direct notice of these controls and our updated terms of service to people around the world (including in the U.S.), allowing people to choose whether or not to enable or disable these settings or to consent to our updated terms. The controls and settings that Facebook is enabling as part of GDPR are available to people around the world, including settings for controlling our use of face recognition on Facebook and for controlling our ability to use data we collect off Facebook Company Products to target ads.

Question 4. The European Union's deadline for full implementation of their General Data Protection Regulations (GDPR) is May 25, 2018. While you have said publically that Facebook plans to extend General Data Protection Regulations (GDPR) across its platform "in spirit," including to users in the U.S., recent media reporting suggests that Facebook's commitment to GDPR implementation across its platform is questionable. In your view, what does implementation of GDPR "in spirit" mean? If Facebook were to be found violating GDPR protections for non-European Union users, what recourse do those users have, legal or otherwise, to remedy a complaint?

Answer. As a part of our overall approach to privacy, we are providing the same tools for access, rectification, erasure, data portability and others to people in the U.S. (and globally) that we provide in the European Union under the GDPR. The controls and settings that Facebook is enabling as part of GDPR include settings for controlling our use of face recognition on Facebook and for controlling our ability to use data we collect off Facebook Company Products to target ads. We recently began providing direct notice of these controls and our updated terms to people around the world (including in the U.S.), allowing people to choose whether or not to enable or disable these settings or to consent to our updated terms. Many of these tools (like our Download Your Information tool, ad preferences tool, and Activity Log) have been available globally for many years.

The substantive protections in our user agreements offered by Facebook Ireland and Facebook, Inc. are the same. However, there are certain aspects of our Facebook Ireland Data Policy that are specific to legal requirements in the GDPR—such as the requirement that we provide contact information for our EU Data Protection Officer or that we identify the "legal bases" we use for processing data under the GDPR. Likewise, our Facebook Ireland terms and Data Policy address the lawful basis for transferring data outside the EU, based on legal instruments that are applicable only to the EU. And other provisions of the GDPR itself pertain to interactions between European regulators and other matters that are not relevant to people located outside of the EU.

Facebook is subject to ongoing oversight by the Federal Trade Commission with respect to its privacy commitments to people and its implementation of privacy settings, under a Consent Order with the FTC. Facebook is subject to the authority of the Irish Data Protection Commissioner, its lead regulator, under the GDPR in the European Union.

Question 5. As reported by Politico on April 17, 2018, Facebook has enlisted the help of conservative organizations to push back against GDPR and other potential regulatory efforts in the U.S. Is Facebook coordinating with political organizations to consider or address potential state or Federal regulatory actions?

Answer. When the GDPR was finalized, we realized it was an opportunity to invest even more heavily in privacy. We not only wanted to comply with the law, but also go beyond our obligations to build new and improved privacy experiences for everyone on Facebook. To that end, as we often do, we sought feedback from people with a variety of perspectives on privacy, including people who use our services, regulators and government officials, privacy and policy experts, and designers. We are applying the same protections, controls, and transparency to people in the U.S. and around the world that we are providing to people in Europe under GDPR.

RESPONSE TO WRITTEN QUESTIONS SUBMITTED BY HON. MAGGIE HASSAN TO MARK ZUCKERBERG

Question 1. During the hearing, you stated that you "don't know" whether Facebook employees actively coordinated with Cambridge Analytica as a result of the support Facebook provided directly to the Trump campaign. Representatives from the Trump campaign have extensively detailed how Facebook provided "hands-on" support to the campaign, embedding Facebook employees at the campaign's digital operation center in San Antonio.[5] Cambridge Analytica appears to have had employees nearby, in the same office, at the same time that Facebook employees were embedded there.

- Was Facebook aware that Cambridge Analytica personnel would be working out of the same Trump campaign office before Facebook agreed to provide support to the campaign at this location? If not, when did someone at Facebook become aware, and what disclosure process was followed internally?
- Would Facebook have still provided support if it knew beforehand that it would be working alongside Cambridge Analytica? Once Facebook found out it would be working alongside Cambridge Analytica, what actions did Facebook take?
- Have you conducted an internal investigation into the vetting process behind this arrangement with the Trump campaign?

Answer. While no one from Facebook was assigned full-time to the Trump campaign, Facebook employees did interact with Cambridge Analytica employees. While our investigation is ongoing, our review indicates that Facebook employees did not identify any issues involving the improper use of Facebook data in the course of their interactions with Cambridge Analytica during the 2016 U.S. Presidential campaign.

In general, political data firms working on the 2016 campaign had access to Facebook's advertising support services, including technical support, and best practices guidance on how to optimize their use of Facebook. Everyone had access to the same tools, which are the same tools that every campaign is offered.

Question 2. You stated that Facebook only collected text/call data when people opted-in from Facebook Messenger. Some reports[6] seem to contradict that, with users who reportedly did not download the Messenger app onto a given device seeing their message data from those devices in their Facebook files. Can you clarify this discrepancy?

You also stated that this was done to improve the user experience. Can you explain why it would be necessary to collect not only the contact data from a user's phone, but also the date, time, and length of calls and store that data for years?

Answer. Call and text history logging is part of an opt-in feature that lets people import contact information to help them connect with people they know on Facebook and Messenger. We introduced the call and text history component of this feature for Android users several years ago, and currently offer it in Messenger and Facebook Lite, a lightweight version of Facebook, on Android.

Contact importers are fairly common among social apps and serve as a way to more easily find the people users want to connect with. They help users find and stay connected with the people they care about and provide them with a better experience across Facebook.

Before we receive call and text history from people, they specifically grant us permission to access this data on their device and separately agree to use the feature. If, at any time, they no longer wish to use this feature they can turn it off, and all previously shared call and text history shared via that app is deleted. People can also access information they previously imported through the Download Your Information tool.

We've reviewed this feature to confirm that Facebook does not collect the content of messages—and will delete all logs older than one year. In the future, people will only upload to our servers the information needed to offer this feature—not broader data such as the time of calls.

Question 3. You stated that information sent via WhatsApp is not seen or collected by Facebook, and is never used to inform advertisements. WhatsApp features end-to-end encryption, meaning Facebook has no access to those messages. But other Facebook services such as Messenger or messages on Instagram are not

---

[5] *https://qz.com/1233579/facebook-and-cambridge-analytica-worked-side-by-side-at-a-trump-campaign-office-insan-antonio/*

[6] *https://arstechnica.com/information-technology/2018/03/facebook-scraped-call-text-message-data-for-years-fromandroid-phones/*

encrypted this way, meaning Facebook does have access to them. Are the content of messages sent through Facebook Messenger or Instagram ever used, or have they ever been used, to inform the placement of advertisements?

Answer. Facebook does not analyze the content of photos or text in users' posts or messages to target ads to them using AI or otherwise. Instead, there are a few primary ways that we personalize the ads and sponsored content for people on Facebook, based on:

- *Information from people's use of Facebook.* When people use Facebook, they can choose to share things about themselves like their age, gender, hometown, or interests. They can also click or like posts, Pages, or articles. We use this information to understand what users might be interested in and hopefully show them ads that are relevant. If a bike shop comes to Facebook wanting to reach female cyclists in Atlanta, we can show their ad to women in Atlanta who liked a Page about bikes. People can always see the "interests" assigned to them in their ad preferences, and if they want, remove them.
- *Information that an advertiser shares with us (or "custom audiences").* In this case, advertisers bring us the customer information so they can reach those people on Facebook. These advertisers might have people's e-mail address from a purchase users made, or from some other data source. If we have matching e-mail addresses, we can show those people ads from that advertiser (although we cannot see the e-mail addresses which are sent to us in hashed form, and these are deleted as soon as we complete the match). In ad preferences people can see which advertisers with their contact information are currently running campaigns—and they can click the top right corner of any ad to hide all ads from that business.
- *Information that websites and apps send to Facebook.* Some of the websites and apps people visit may use Facebook tools to make their content and ads more relevant, if people consent to let Facebook show them ads based on data from third-party partners. For example, if an online retailer is using Facebook Pixel, they can ask Facebook to show ads to people who looked at a certain style of shoe or put a pair of shoes into their shopping cart. If users don't want this data used to show them ads, they can turn it off in ad preferences.
- *Facebook also offers Lookalike Audiences.* Advertisers creating a Lookalike Audience choose a source audience (which could include a custom audience as described above, people who have opened or completed a form in lead ads on Facebook, people who have interacted with the advertiser's Facebook page or its Instagram profile). Facebook then identifies common qualities of the people in the source audience (*e.g.,* demographic information or information about their interests), and then identifies people who are similar to them (on the basis of the common signals identified in the source audience), without sharing this information with the advertiser.

Question 4. What research have you done relating to users' understanding of your policies and/or procedures relating to privacy and/or security of user data?

Answer. We do extensive research around our privacy controls, including focus-groups and on-platform surveys. Our research overwhelmingly demonstrates that, while "up front" information like that contained in the terms of service are useful, in-product controls and education are the most meaningful to people and the most likely to be read and understood. On-demand controls are also important, and we recently redesigned our entire settings menu on mobile devices from top to bottom to make things easier to find. We also created a new Privacy Shortcuts, a menu where people can control their data in just a few taps, with clearer explanations of how our controls work. The experience is now clearer, more visual, and easy-to-find.

Improving people's understanding of how digital services work is an industry-wide challenge that we are highly committed to addressing. That's why, over the last 18 months, we've run a global series of design workshops called "Design Jams", bringing together experts in design, privacy, law, and computer science to work collaboratively on new and innovative approaches. These workshops have run in Paris, London, Dublin, Berlin, Sao Paolo, Hong Kong, and other cities, and included global regulators and policymakers. At these workshops, expert teams use "people centric design" methods to create innovative new design prototypes and experiences to improve transparency and education in digital services. These workshops inform Facebook's constantly-improving approach.

In recognition of the need for improved approaches to data transparency across all digital services, working with partners from academia, design, and industry we recently launched TTC Labs, a design innovation lab that seeks to improve user experiences around personal data. TTC Labs is an open platform for sharing and inno-

vation and contains insights from leading experts in academia, design, and law, in addition to prototype designs from the Design Jams, template services and open-source toolkits for people-centric design for transparency, trust and control of data. Working collaboratively, and based on open-source approaches, TTC Labs seeks to pioneer new and more people-centric best practices for people to understand how their data is used by digital services, in ways that they find easy to understand and control.

Facebook is highly committed to improving people's experience of its own services as well as in to support improvements across the industry.

Question 5. What percentage of users change their default privacy settings?

Answer. There is no single number that measures how much time people spend understanding how Facebook services work, in large part because Facebook seeks, as much as possible, to put controls and information in context within its service.

We've heard loud and clear that privacy settings and other important tools are hard to find and that we must do more to keep people informed. So, we're taking additional steps to put people more in control of their privacy. For instance, we redesigned our entire settings menu on mobile devices from top to bottom to make things easier to find. We also created a new Privacy Shortcuts in a menu where users can control their data in just a few taps, with clearer explanations of how our controls work. The experience is now clearer, more visual, and easy-to-find. Furthermore, we also updated our terms of service that include our commitments to everyone using Facebook. We explain the services we offer in language that's easier to read. We also updated our Data Policy to better spell out what data we collect and how we use it in Facebook, Instagram, Messenger, and other products.

Question 6. What types of data or information does Facebook collect and store about non-Facebook users? For what purpose does Facebook collect this data and information?

Answer. When people visit apps or websites that feature our technologies—like the Facebook Like or Comment button—our servers automatically log (i) standard browser or app records of the fact that a particular device or user visited the website or app (this connection to Facebook's servers occurs automatically when a person visits a website or app that contains our technologies, such as a Like button, and is an inherent function of Internet design); and (ii) any additional information the publisher of the app or website chooses to share with Facebook about the person's activities on that site (such as the fact that a purchase was made on the site). This is a standard feature of the Internet, and most websites and apps share this same information with multiple different third-parties whenever people visit their website or app. For example, the House Energy and Commerce Committee's website shares information with Google Analytics to help improve the site. This means that, when a person visits the Committee's website, it sends browser information about their visit to that party. More information about how this works is available at *https://newsroom.fb.com/news/2018/04/data-off-facebook/*.

When the person visiting a website featuring Facebook's tools is not a registered Facebook user, Facebook does not have information identifying that individual, and it does not create profiles for this individual.

We use the browser and app logs that apps and websites send to us—described above—in the following ways for non-Facebook users. First, these logs are critical to protecting the security of Facebook and to detecting or preventing fake account access. For example, if a browser has visited hundreds of sites in the last five minutes, that's a sign the device might be a bot, which would be an important signal of a potentially inauthentic account if that browser then attempted to register for an account. Second, we aggregate those logs to provide summaries and insights to websites and apps about how many people visit or use their product or use specific features like our Like button—but without providing any information about a specific person. We do not create profiles for non-Facebook users, nor do we use browser and app logs for non-Facebook users to show targeted ads from our advertisers to them or otherwise seek to personalize the content they see. However, we may take the opportunity to show a general ad that is unrelated to the attributes of the person or an ad encouraging the non-user to sign up for Facebook.

We do receive some information from devices and browsers that may be used by non-users. For example:

- We also may receive information about the device of a non-registered user if that user visits a part of Facebook that does not require people to log in—such as a public Facebook Page. The information we log when people visit our websites or apps is the same as described above and is the same information that any provider of an online service would receive.

- In addition, Facebook may receive some basic information about devices where Facebook apps are installed, including before people using those devices have registered for Facebook (such as when a user downloads a Facebook app, but has not yet created an account, or if the app is preloaded on a given device). This device data includes things like device model, operating system, IP address, app version and device identifiers. We use this information to provide the right version of the app, help people who want to create accounts (for example, optimizing the registration flow for the specific device), retrieving bug fixes and measuring and improving app performance. We do not use this information to build profiles about non-registered users.

Question 7. Some reports have indicated that private messages sent via Facebook may have been accessible to Cambridge Analytica and other third party developers via the first version of the Graph API.[7] Is there merit to those reports? If so, how many users' private messages would have been available through this mechanism?

Answer. At the outset, we do not know what data Kogan may have shared with Cambridge Analytica. Our investigation into these matters is ongoing, and we are paused on investigating Cambridge Analytica directly (or conducting a forensic audit of its systems) due to the request of the UK Information Commissioner's Office, which is separately investigating Cambridge Analytica, a UK entity. The best information to date also suggests only U.S. user data was shared by Kogan with Cambridge Analytica.

Approximately 300,000 Facebook users worldwide installed Kogan's app. For the majority of these users, the app requested consent to access the following data fields associated with the user and with the friends of the user: Public profile data, including name and gender; Birthdate; "Current city" in the "About" section of the user's profile, if provided; and Facebook Pages liked.

For a small subset of users, it appears that the app also requested consent to access users' Facebook messages (fewer than 1,500 individuals, based on current information) and to posts that appeared in the user's News Feed or Timeline (approximately 100 individuals, based on current information)—but only for users who installed the app. For a small subset of users (fewer than 1,500 individuals, based on current information), it appears that the app also requested consent to access the hometowns that the users' friends had specified in the "About" section of their profiles. And for a handful of people (fewer than 10) who appear to be associated with Kogan/GSR, the app requested consent to e-mail address and photos.

Question 8. What steps is Facebook taking to combat the opioid crisis (such as efforts to crack down on the sale of illicit drugs or identify users at risk of addiction)?

Answer. Thank you for highlighting this important issue. We have an iterative, proactive process to help prevent opportunities for—and respond quickly to—illicit drug sales on our platforms:

- Our Community Standards make it very clear that buying, selling or trading non-medical or pharmaceutical drugs is not allowed on Facebook. Any time we become aware of content on Facebook that is facilitating activity like drug sales, we remove it and have taken numerous measures to minimize the opportunity for these activities to take place on our platform.
- We make it easy for people to flag content for us so that we can quickly review and remove it if it violates. That's why people can report any piece of content on Facebook—profiles, Pages, Groups, individual content and even comments.
- If we identify violating content, we are able to look for associated profiles, Pages, groups, and accounts and remove them.
- We have also made it harder for people to find content that facilitates the sale of opioids on our platform.
- We have removed content that violated our policies that was surfaced in Search.
- We have blocked hundreds of terms associated with drugs sales from being able to surface results on Facebook or only returning links to news about drugs shared for awareness.
- We have removed thousands of terms from being suggested in search—meaning that our systems won't recognize the beginning of the word as it is being typed and suggest what the completed term to search is.
- We continue to look for ways to get faster at finding and removing this content, working across our policy, operations, product, and partnerships team. We also

[7] *https://medium.com/tow-center/the-graph-api-key-points-in-the-facebook-and-cambridge-analytica-debacle-b69fe692d747*

update our detection methods as bad actors work to game the system and bypass our safeguards.

We recently launched a new feature on Facebook so that now, when people search for help with opioid misuse—as well as attempt to buy opioids—they are prompted with content at the top of the search results page that will ask them if they would like help finding free and confidential treatment referrals. This will then direct them to the Substance Abuse and Mental Health Services Administration National Helpline.

The same resources will be available on Instagram in the coming weeks. This is one of a number of ways we are helping connect people with resources and communities to support them.

Question 9. What process does Facebook use to vet third parties before granting them access to user data?

Answer. In April 2014, we announced that we would more tightly restrict our platform APIs to prevent abuse. At that time, we made clear that existing apps would have a year to transition—at which point they would be forced (1) to migrate to the more restricted API and (2) be subject to Facebook's new review and approval protocols. The vast majority of companies were required to make the changes by May 2015; a small number of companies (fewer than 100) were given a one-time extension of less than six months beyond May 2015 to come into compliance. (One company received an extension to January 2016.) In addition, in the context of our ongoing review of third-party apps, we discovered a very small number of companies (fewer than 10) that theoretically could have accessed limited friends' data as a result of API access that they received in the context of a beta test. We are not aware that any of this handful of companies used this access, and we have now revoked any technical capability they may have had to access any friends' data.

New apps that launched after April 30, 2014 were required to use our more restrictive platform APIs. We required apps seeking additional categories of data to undergo proactive review by our internal teams. We rejected more than half of the apps seeking these permissions, including the second version of Kogan's app.

We review apps to ensure that the requested permissions clearly improve the user experience and that the data obtained is tied to an experience within the app. We conduct a variety of manual and automated checks of applications on the platform for Policy compliance, as well as random sampling. When we find evidence of or receive allegations of violations, we investigate and, where appropriate, employ a number of measures, including restricting applications from our platform, preventing developers from building on our platform in the future, and taking legal action where appropriate.

Recently, we announced a number of additional steps we're taking to address concerns raised by Kogan's app.

- *Review our platform.* We will investigate all apps that had access to large amounts of data before the platform changes we announced in 2014, and we will audit any app where we identify suspicious activity. If we identify misuses of data, we'll take immediate action, including banning the app from our platform and pursuing legal action if appropriate.
- *Tell people about data misuse.* We will tell people about apps that have misused their data. This includes building a way for people to know if their data might have been accessed via the app. Moving forward, if we remove an app for misusing data, we will tell everyone who used it.
- *Turn off access for unused apps.* If someone has not used an app within the last three months, we will turn off the app's access to their data.
- *Restrict Facebook Login data.* We are changing Login, so that the only data that an app can request without app review will include name, profile photo, and e-mail address. Requesting any other data will require approval from Facebook. We will also no longer allow apps to ask for access to information like religious or political views, relationship status and details, custom friends lists, education and work history, fitness activity, book reading and music listening activity, news reading, video watch activity, and games activity. We will encourage people to manage the apps they use. We already show people what apps their accounts are connected to and allow them to control what data they've permitted those apps to use. But we're making it easier for people to see what apps they use and the information they have shared with those apps.
- *Reward people who find vulnerabilities.* We launched the Data Abuse Bounty program so that people can report to us any misuses of data by app developers.

- *Update our policies.* We have updated our terms and Data Policy to explain how we use data and how data is shared with app developers.

Question 10. What steps does Facebook take to monitor third parties who have access to user data?

Answer. See Response to Question 9.

Question 11. Which third parties have improperly accessed or inappropriately used user data, or violated signed agreements with Facebook regarding data? What steps has Facebook taken to remedy these events?

Answer. Facebook is in the process of investigating all the apps that had access to large amounts of information, such as extensive friends data (if those friends privacy data settings allowed sharing), before we changed our platform policies in 2014—significantly reducing the data apps could access. Where we have concerns about individual apps, we are investigating them—and any app that either refuses or fails an audit will be banned from Facebook. As of early June 2018, thousands of apps have been investigated and around 200 have been suspended—pending a thorough investigation into whether they did in fact misuse any data.

These apps relate to a handful of developers: Kogan, AIQ, Cube You, the Cambridge Psychometrics Center, and myPersonality, with many of the suspended apps being affiliated with the same entity. Many of these apps also appear to be "test" apps that were never released to the public, and therefore would not have acquired significant user data, although our investigation into these apps is ongoing.

Question 12. You stated that Facebook is an "idealistic company." Facebook has reportedly sought to build a censorship-friendly app to help enter the Chinese market.[8] Are those reports true? If so, do you consider those actions to be consistent with Facebook's idealism?

Answer. Because Facebook has been blocked in China since 2009, we are not in a position to know exactly how the government would seek to apply its laws and regulations on content were we permitted to offer our service to Chinese users. Since 2013, Facebook has been a member of the Global Network Initiative (GNI), a multi-stakeholder digital rights initiative. As part of our membership, Facebook has committed to the freedom of expression and privacy standards set out in the GNI Principles—which are in turn based on the Universal Declaration of Human Rights and the United Nations Guiding Principles on Business and Human Rights—and we are independently assessed on our compliance with these standards on a biennial basis.

In keeping with these commitments, rigorous human rights due diligence and careful consideration of free expression and privacy implications would constitute important components of any decision on entering China.

Question 13. We are all grappling with the ability of foreign nations to exploit technology platforms like Facebook to spread propaganda and misinformation. While Facebook does not operate within China, reports have shown that the Chinese government advertises extensively on Facebook to spread propaganda in the U.S. and throughout Southeast Asia. Reports indicate that the Chinese government is the largest advertiser Facebook has in Asia. Do you believe Facebook should be a platform for allowing foreign nations to spread propaganda? Are the Chinese government's propaganda efforts consistent with Facebook's goal of cracking down on misinformation?

Answer. Entities can maintain a presence on Facebook as long as they comply with Facebook's policies, including complying with applicable law. We hold all accounts to the same standards, including standards related to authenticity, and we remove accounts and content that violate our policies. For content that does not violate our policies but that is false or misleading, we have begun to work with third-party fact-checking organizations to provide additional information to people who see or share this kind of content. Posts that don't violate Facebook's policies but that are determined to be false or disputed may also appear lower in News Feed and become less likely to be widely distributed. If we become aware that our policies are being violated, we will take action.

We've made important changes to prevent bad actors from using misinformation to undermine the democratic process. Here is a list of the 10 most important changes we have made:

- *Ads transparency.* Advertising should be transparent: users should be able to see all the ads an advertiser is currently running on Facebook, Instagram and Messenger. And for ads with political content, we've created an archive that will hold ads with political content for seven years—including information about ad

[8] *https://www.nytimes.com/2016/11/22/technology/facebook-censorship-tool-china.html*

impressions and spend, as well as demographic data such as age, gender, and location. People in Canada and Ireland have already been able to see all the ads that a Page is running on Facebook—and we've launched this globally.

- *Verification and labeling.* Every advertiser will now need confirm their ID and location before being able to run any ads with political content in the U.S. All ads with political content will also clearly state who paid for them.
- *Updating targeting.* We want ads on Facebook to be safe and civil. We thoroughly review the targeting criteria advertisers can use to ensure they are consistent with our principles. As a result, we removed nearly one-third of the targeting segments used by the IRA. We continue to allow some criteria that people may find controversial. But we do see businesses marketing things like historical books, documentaries or television shows using them in legitimate ways.
- *Better technology.* Over the past year, we've gotten increasingly better at finding and disabling fake accounts. We now block millions of fake accounts each day as people try to create them—and before they've done any harm. This is thanks to improvements in machine learning and artificial intelligence, which can proactively identify suspicious behavior at a scale that was not possible before—without needing to look at the content itself.
- *Action to tackle fake news.* We block millions of fake account attempts each day as people try to create them thanks to improvements in machine learning and artificial intelligence. We are also working hard to stop the spread of false news. To reduce the spread of false news, we remove fake accounts and disrupt economic incentives for traffickers of misinformation. We also use various signals, including feedback from our community, to identify potential false news. In countries where we have partnerships with independent third-party fact-checkers, stories rated as false by those fact-checkers are shown lower in News Feed. If Pages or domains repeatedly create or share misinformation, we significantly reduce their distribution and remove their advertising rights.
- *Significant investments in security.* We're doubling the number of people working on safety and security from 10,000 last year to over 20,000 this year. We expect these investments to impact our profitability. But the safety of people using Facebook needs to come before profit.
- *Industry collaboration.* Recently, we joined 34 global tech and security companies in signing a TechAccord pact to help improve security for everyone.
- *Information sharing and reporting channels.* In the 2017 German elections, we worked closely with the authorities there, including the Federal Office for Information Security (BSI). This gave them a dedicated reporting channel for security issues related to the Federal elections.
- *Tracking 40+ elections.* In recent months, we've started to deploy new tools and teams to proactively identify threats in the run-up to specific elections. We first tested this effort during the Alabama Senate election, and plan to continue these efforts for elections around the globe, including the U.S. midterms. Last year we used public service announcements to help inform people about fake news in 21 separate countries, including in advance of French, Kenyan and German elections.
- *Action against the Russia-based IRA.* In April, we removed 70 Facebook and 65 Instagram accounts—as well as 138 Facebook Pages—controlled by the IRA primarily targeted either at people living in Russia or Russian-speakers around the world including from neighboring countries like Azerbaijan, Uzbekistan, and Ukraine. The IRA has repeatedly used complex networks of inauthentic accounts to deceive and manipulate people in the U.S., Europe and Russia—and we don't want them on Facebook anywhere in the world.

We are taking steps to enhance trust in the authenticity of activity on our platform, including increasing ads transparency, implementing a more robust ads review process, imposing tighter content restrictions, and exploring how to add additional authenticity safeguards.

Question 14. You have stated that users are able to download all of the data that Facebook has about them. Does this include data that Facebook has obtained through means such as cross-web tracking, purchasing data from brokers, and inferential data created with that user data?

If not, how can a user access this data?

Answer. Every user has a dedicated section in their settings which enables them to access or download their information at any time. Our Download Your Information or "DYI" tool is Facebook's data portability tool and was launched many years ago to let people access and download many types of information that we maintain

about them. The data in DYI and in our Ads Preferences tool contain each of the interest categories that are used to show people ads, along with information about the advertisers that are currently running ads based on their use of an advertiser's website or app. People also can choose not to see ads from those advertisers. We recently expanded the tools we provide people for accessing their information, which will now allow people to see their data, delete it, and easily download and export it. More information is available at *https://newsroom.fb.com/news/2018/04/new-privacy-protections/*.

Responding to feedback that we should do more to provide information about websites and apps that send us information when people use them, we also announced plans to build Clear History. This new feature will enable users to see the websites and apps that send us information when they use them, clear this information from their account, and turn off Facebook's ability to store it associated with their account going forward.

We have also introduced Access Your Information. This feature provides a new way for people to access and manage their information. Users can go here to delete anything from their timeline or profile that they no longer want on Facebook. They can also see their ad interests, as well as information about ads they've clicked on and advertisers who have provided us with information about them that influence the ads they see. From here, they can go to their ad settings to manage how this data is used to show them ads.

Question 15. Before the hearing, Facebook announced an independent election research commission to solicit research on the effects of social media on elections and democracy. Does Facebook plan to solicit similar research on the effects of social media on other important aspects of society, including privacy, mental health and wellbeing, inequality, etc.?

Answer. Facebook employs social psychologists, social scientists, and sociologists, and collaborates with top scholars to better understand well-being. Facebook has also pledged $1 million towards research to better understand the relationship between media technologies, youth development and well-being. Facebook is teaming up with experts in the field to look at the impact of mobile technology and social media on kids and teens, as well as how to better support them as they transition through different stages of life. Facebook is committed to bringing people together and supporting well-being through meaningful interactions on Facebook.

Question 16. Many large institutions have set up independent systems to ensure transparency and internally check bad decisions. Federal agencies have inspectors general and offices to encourage whistleblowing. Many companies have ombudsmen, and some media companies have public editors to help publicly examine and evaluate their choices. Hospitals have ethics boards. What kinds of independent systems does Facebook have? Have you considered setting up an independent entity to help publicly examine and explain your decision-making?

Answer. Facebook's Board of Directors acts as the management team's adviser and monitors management's performance. The Board also reviews and, if appropriate, approves significant transactions and develops standards to be utilized by management in determining the types of transactions that should be submitted to the Board for review and approval or notification. The Board of Directors also has an Audit and Risk Oversight Committee with an oversight role.

In addition to the Board's role, Facebook works with outside groups on these issues. For example, Relman, Dane & Colfax, a respected civil rights law firm, will carry out a comprehensive civil rights assessment of Facebook's services and internal operations. Laura Murphy, a national civil liberties and civil rights leader, will help guide this process—getting feedback directly from civil rights groups, like The Leadership Conference on Civil and Human Rights, and help advise Facebook on the best path forward.

Moreover, Facebook recently announced a new initiative to help provide independent, credible research about the role of social media in elections, as well as democracy more generally. It will be funded by the Laura and John Arnold Foundation, Democracy Fund, the William and Flora Hewlett Foundation, the John S. and James L. Knight Foundation, the Charles Koch Foundation, the Omidyar Network, and the Alfred P. Sloan Foundation. At the heart of this initiative will be a group of scholars who will:

- Define the research agenda;
- Solicit proposals for independent research on a range of different topics; and
- Manage a peer review process to select scholars who will receive funding for their research, as well as access to privacy-protected datasets from Facebook which they can analyze.

Facebook will not have any right to review or approve the r research findings prior to publication. More information regarding the study is available at *https://newsroom.fb.com/news/2018/04/new-elections-initiative/*.

Question 17. When Facebook comes across terrorist-related content—such as ISIS or al-Qaeda propaganda—does Facebook proactively alert Federal law enforcement to the terrorist content? If not, under what circumstances will Facebook alert Federal law enforcement about terrorist propaganda on your platform?

Answer. We reach out to law enforcement if we learn of content that we believe reflects a credible threat of imminent harm. We have been able to provide support to authorities around the world that are responding to the threat of terrorism, including in cases where law enforcement has been able to disrupt attacks and prevent harm. Further, as part of official investigations, government officials sometimes request data about people who use Facebook. We have strict processes in place to handle these government requests, and we disclose account records in accordance with our terms of service and applicable law. We publish more information in our Law Enforcement Guidelines at *https://www.facebook.com/safety/groups/law/guidelines/* and Transparency Report at *https://transparency.facebook.com/*.

Question 18. The other question I had, and it does not just apply to Facebook, is should the framework include financial penalties when large providers like Facebook are breached and privacy is compromised as a result? There is very little incentive for whether it is Facebook or Equifax to actually be abreast of protecting customer privacy and working for potential breaches or vulnerabilities in the system.

Answer. Protecting people's data is one of our most important responsibilities. We know that if people don't trust that their information will be safe on Facebook, they won't feel comfortable using our services.

We have every incentive to work as hard as we can to protect people's information, and we're committed to continuing our work to improve those protections.

Facebook is generally open to the idea of Federal breach notification requirements, particularly legislation that would centralize reporting and ensure a consistent approach across the United States. For example, in Europe, the GDPR requires notification to a lead supervisory authority, rather than individual member states, in cases of a data breach. In the United States, however, there is no centralized notification scheme, and instead, reporting obligations vary widely across all 50 states. This complexity makes it harder to respond appropriately and swiftly to protect people in the event of a data breach. We believe this is an important issue and an area that is ripe for thoughtful regulation.

Facebook is generally not opposed to regulation but wants to ensure it is the right regulation. We are already regulated in many ways—for example, under the Federal Trade Commission Act—and we are subject to ongoing oversight by the FTC under the terms of a 2011 consent order. Facebook has inherent incentives to protect its customers' privacy and address breaches and vulnerabilities. Indeed, the recent discovery of misconduct by an app developer on the Facebook platform clearly hurt Facebook and made it harder for us to achieve our social mission. As such, Facebook is committed to protecting our platform from bad actors, ensuring we are able to continue our mission of giving people a voice and bringing them closer together.

We are also actively building new technologies to help prevent abuse on its platform, including advanced AI tools to monitor and remove fake accounts. We have also significantly increased our investment in security, employing more than 15,000 individuals working solely on security and content review and planning to increase that number to over 20,000 by the end of the year. We have also strengthened our advertising policies, seeking to prevent discrimination while improving transparency.

Response to Written Questions Submitted by Hon. Catherine Cortez Masto to Mark Zuckerberg

Question 1. Children's Data: Does Instagram have an age limit requirement similar to the 13 years old Facebook requires?

Answer. Yes, Instagram requires everyone to be at least 13 years old before they can create an account (and in some jurisdictions, this age limit may be higher).

Question 2. How vulnerable or widely utilized have children's (18 or younger) data been in both Facebook and your other platforms?

Answer. We take the privacy, safety, and security of all those who use our platform very seriously, and when it comes to minors (13 to 18 years old), we provide special protections and resources.

We also provide special protections for teens on Facebook and Messenger. We provide education before allowing teens to post publicly. We don't show search results based on specific profile data (high school, birthday/age, and hometown, or current city) of teens to unconnected adults when the adults search on Facebook. Unconnected adults can't message minors who are 13–17. And, we prohibit search engines off Facebook from indexing minors' profiles. And, we have age limits for advertisements. For example, ads for dating sites, financial services, and other products or services are gated to users under 18.

We provide special resources to help ensure that they enjoy a safe and secure experience. For example, we recently announced the launch of our Youth Portal, which is available in 60 languages at *https://www.facebook.com/safety/youth*. This portal is a central place for teens that includes:

- *Education.* Information on how to get the most out of products like Pages, Groups, Events, and Profile, while staying safe. Plus, information on the types of data Facebook collects and how we use it.
- *Peer Voices.* First-person accounts from teens around the world about how they are using technology in new and creative ways.
- *Ways to control user experience.* Tips on things like security, reporting content, and deciding who can see what teens share.
- *Advice.* Guidelines for how to safely get the most out of the internet.

Instagram also will be providing information to teens to show them where they can learn about all of the tools on Instagram to manage their privacy and stay safe online, including how to use the new Access and Download tools to understand what they have shared online and learn how to delete things they no longer want to share. We are also making this information available in formats specifically designed for young users, including video tutorials for our privacy and safety tools, and teen-friendly FAQs about the Instagram Terms of Use, Data Policy, safety features, and Community Guidelines.

Instagram has also launched new content on Instagram Together, including videos and FAQs about privacy controls; information on how to use safety features, including comment controls, blocking accounts, reporting abuse, spam, or troubling messages; information on responsible social media use; and FAQs about safety on Instagram. We will be reaching out to users under 18 on Instagram to encourage them to learn more on Instagram Together, available at *https://www.instagram-together.com/*.

Further, we have content restrictions and reporting features for everyone, including minors. We have Community Standards that prohibit hate speech, bullying, intimidation, and other kinds of harmful behavior. We encourage people to report posts and rely on our team of content reviewers around the world to review reported content. Our reviewers are trained to look for violations and enforce our policies consistently and as objectively as possible. When reviewed by our team, we hide certain graphic content from users under 18 (and include a warning for adults). We are also working to improve our ability to get our community help in real time, especially in instances where someone is expressing thoughts of suicide or self-harm, by expanding our use of proactive detection, working with safety experts and first-responders, and dedicating more reviewers from our Community Operations team.

Question 3. How many children (18 or younger) had their data taken during the Cambridge Analytica breach?

Answer. The Children's Online Privacy Protection Act (COPPA) requires parental consent and notification in specific instances involving the collection and use of data about children under the age of 13. Facebook does not allow children under the age of 13 on its service or collect data about children under 13 that would trigger parental consent or notification.

Question 4. Are you notifying parents about their children's exposed data?

Answer. See Response to Question 3.

Question 5. Discriminatory Advertising: Please provide a detailed description, including screenshots if applicable, of the nondiscrimination compliance certification that Facebook currently requires advertisers to complete.

Answer. Please refer to our letter to you dated May 16, 2018.

Question 6. Please provide a complete list of the characteristics, categories, descriptors, and/or interests that Facebook allows advertisers to select in order to target certain users for inclusion in an advertisement's audience.

Answer. Please refer to our letter to you dated May 16, 2018. Please note, however, that in limited cases and for the purpose of running ads that are not related to housing, employment or credit, we are re-enabling the ability of advertisers to

exclude people from their audiences based on family status but are reviewing this as a targeting option.

Question 7. Please provide a complete list of the characteristics, categories, descriptors, and/or interests that Facebook allows advertisers to select in order to exclude certain users from an advertisement's audience.

Answer. See Response to Question 6.

Question 8. Are there any characteristics, categories, descriptors, and/or interests that

Facebook had previously permitted advertisers to select, but that Facebook no longer allows to be selected as targeting or exclusion criteria? If so, please provide a complete list of those characteristics, categories, descriptors, and/or interests.

Answer. See Response to Question 6.

Question 9. Are there certain characteristics, categories, descriptors, and/or interests that Facebook has never allowed advertisers to select for the purpose of targeting or excluding users from an advertisement's audience? If so, please provide a complete list of those characteristics, categories, descriptors, and/or interests.

Answer. See Response to Question 6.

Question 10. Please describe the process that Facebook uses to determine whether a characteristic, category, descriptor, or interest will be available for selection as a targeting or exclusion criteria. If Facebook has a written policy governing this determination, please provide a copy.

Answer. We have Community Standards that prohibit hate speech, bullying, intimidation, and other kinds of harmful behavior. We hold advertisers to even stricter advertising policies to protect users from things like discriminatory ads. We don't want advertising to be used for hate or discrimination, and our policies reflect that. For example, our Advertising Policies make it clear that advertisers may not discriminate against people based on personal attributes such as race, ethnicity, color, national origin, religion, age, sex, sexual orientation, gender identity, family status, disability, and medical or genetic condition. The Policies also prohibit asserting or implying that a person belongs to one of these groups.

We educate advertisers on our anti-discrimination policy, and when we detect that an advertiser is attempting to run a housing, employment or credit ad, we require the advertiser to certify compliance with our anti-discrimination policy and anti-discrimination laws. We are committed to getting better at enforcing our advertising policies. We review many ads proactively using automated and manual tools, and reactively when people hide, block, or mark ads as offensive. We are taking aggressive steps to strengthen both our automated and our manual review. We are also expanding our global ads review teams and investing more in machine learning to better understand when to flag and take down ads, such as ads that use our multicultural affinity segments in connection with offers of housing, employment or credit opportunities.

Question 11. Regardless of whether the characteristics are described as demographic, behavioral, or interest-based criteria, does Facebook allow employment, housing, credit advertisements to be targeted to users on the basis of protected characteristics, including race, national origin, religion, sex, gender, disability, age, and familial status?

Answer. See Response to Question 6.

Question 12. Regardless of whether the characteristics are described as demographic, behavioral, or interest-based criteria, does Facebook allow advertisers for employment and housing to exclude users on the basis of protected characteristics, including race, national origin, religion, sex, gender, disability, age, and familial status?

Answer. See Response to Question 6.

Question 13. Has Facebook reviewed characteristics/categories available for advertising to select or exclude when targeting that can be used as "proxies" for protected characteristics? If so, what is Facebook's policy regarding the continued availability of that characteristic as a targeting or exclusion criteria and has Facebook ever removed categories that were being used as "proxies" for protected categories? How does Facebook go about determining which such categories could potentially be used as "proxies" for discrimination?

Answer. See Response to Question 10.

Question 14. Does Facebook allow employment, housing, and credit advertisements to be targeted to users on the basis of categories that may be reasonable proxies for protected characteristics?

Answer. See Response to Question 6.

Question 15. Does Facebook allow employment, housing, and credit advertisements to be targeted to users on the basis of their sexual orientation or gender identity?

Answer. Please refer to our letter to you dated May 16, 2018.

Question 16. In Facebook's December 20, 2017 press release, Rob Goldman, VP of Ads, wrote that Facebook "proactively look[s] for bad ads, and investigate[s] concerns when they are raised." Please describe Facebook's process for monitoring ads for possible violations of Title VII, the Fair Housing Act, the Americans with Disabilities Act, and Title II of the Genetic Information Nondiscrimination Act.

Answer. Please refer to our letter to you dated May 16, 2018.

Question 17. Does Facebook "proactively look" for ads that may be discriminatory on the basis of each protected characteristic before they are posted to the platform?

Answer. Please refer to our letter to you dated May 16, 2018.

Question 18. Does Facebook have defined, written policies for determining whether an employment, housing, or credit ad is discriminatory on the basis of each protected characteristic, and a procedure for deleting such ads? If so, please provide copies of such policies.

Answer. Please refer to our letter to you dated May 16, 2018.

Question 19. Has Facebook ever proactively deleted an employment, housing, or credit ad on the grounds that it discriminated on the basis of a protected characteristic? If so, how many such ads has Facebook deleted, broken down by each protected characteristic?

Answer. Please refer to our letter to you dated May 16, 2018.

Question 20. Has Facebook ever deleted an employment, housing, or credit ad on the grounds that it discriminated on the basis of a protected characteristic in response to a user complaint? If so, how many such ads has Facebook deleted, broken down by each protected characteristic?

Answer. Please refer to our letter to you dated May 16, 2018.

Question 21. Has Facebook ever barred a businesses or ad companies from using its services because of discriminatory ads? How many? Please detail the process Facebook has for addressing discriminatory advertisers, once identified.

Answer. Please refer to our letter to you dated May 16, 2018.

Question 22. Many state and local nondiscrimination laws go further than Federal statutes prohibiting discrimination against protected classes. Does Facebook require advertisers to certify that they will comply with state and local nondiscrimination laws?

Answer. Please refer to our letter to you dated May 16, 2018.

Question 23. Does Facebook "proactively look" at employment, housing, and credit ads to evaluate their compliance with state and local nondiscrimination laws?

Answer. Please refer to our letter to you dated May 16, 2018.

Question 24. Does Facebook respond to user complaints about employment, housing, and credit ads that may violate state and local nondiscrimination laws? If so, how?

Answer. Please refer to our letter to you dated May 16, 2018.

Question 25. Please provide a timeline and any relevant documentation of interactions with the U.S. Department of Housing and Urban Development on Facebook's advertisement policies.

Answer. Please refer to our letter to you dated May 16, 2018.

Question 26. Please provide a detailed description of any other U.S. Federal agencies that have contacted Facebook regarding the issue of discriminatory advertising on the Facebook platform.

Answer. We regularly work cooperatively with regulators that may have questions about our platform and are happy to answer questions.

Question 27. Please describe when this contact took place and a detailed description of the agency's inquiry and interaction with Facebook, as well as Facebook's response.

Answer. See Response to Question 26.

Question 28. Will Facebook commit to having an outside entity conducting a Civil Rights Audit of its platform and advertising practices? If so, will Facebook commit to meaningfully consulting civil rights organizations on the perimeters of the Civil Rights Audit? Will Facebook commit to making the results of such audit accessible to the public?

Answer. Relman, Dane & Colfax, a respected civil rights law firm, will carry out a comprehensive civil rights assessment of Facebook's services and internal operations. Laura Murphy, a national civil liberties and civil rights leader, will help

guide this process—getting feedback directly from civil rights groups, like The Leadership Conference on Civil and Human Rights, and help advise Facebook on the best path forward.

Question 29. Discrimination and Diversity in Tech Community: Over the past few months, our country has been reckoning with some hard truths about the way that women and minorities are treated in the workplace. And I think this is a moment for all types of organizations, including tech giants like the one represented here, to take a clear-eyed accounting of their culture and practices, to take responsibility for what hasn't worked, and to renew their commitments to make meaningful improvements. The Equal Employment Opportunity Commission's 2016 report on "Diversity in High Tech" found that that women, African Americans, and Hispanics are all represented at significantly lower levels in high tech than in private industry as a whole. And while recent internal studies by you at Facebook, and Google, have showed some progress in the hiring of women, there has not been equal improvement in the representation of people of color and other underrepresented groups.

What does diversity mean to you, and how do you want it reflected in your operations?

Answer. With a global community of over two billion people on Facebook, greater diversity and inclusivity are critical to achieving our mission. Studies have shown that cognitive diversity on teams that are working on hard problems produces better results. Diversity helps us build better products, make better decisions and better serve our community. In order to achieve that, we have developed programming to attract and retain more people from traditionally underrepresented groups which include women, people of color, veterans and people with disabilities.

We are not where we would like to be, but we are encouraged that representation for people from underrepresented groups at Facebook has increased. We've grown Black and Hispanic representation by 1 percent each (2 percent combined) between our first report in 2014 and our most recent report in 2017:

- Black Representation: from 2 percent to 3 percent
- Hispanic Representation: from 4 percent to 5 percent
- Black Non-Tech: from 2 percent to 6 percent
- Hispanic Non-Tech: from 6 percent to 8 percent
- Black Leadership: from 2 percent to 3 percent
- Hispanic Leadership: from 3 percent to 4 percent
- Black and Hispanic Tech have stayed at 1 percent and 3 percent

As of August 2017, the number of women globally increased from 33 percent to 35 percent:

- Women in Tech: from 17 percent to 19 percent
- Women in Non-Tech: from 47 percent to 55 percent
- Women in Leadership: from 23 percent to 28 percent
- Women made up 27 percent of all new graduate hires in engineering and 21 percent of all new technical hires at Facebook.

We seek to promote diversity in a variety of ways, and we want to highlight three programs in particular. First, we have adopted our Diverse Slate Approach (DSA) to interviewing job candidates. The more people that hirers interview who don't look or think like them, the more likely they are to hire someone from a diverse background. To hardwire this behavior at Facebook, we introduced our DSA in 2015 and have since rolled it out globally. DSA sets the expectation that hiring managers will consider candidates from underrepresented backgrounds when interviewing for an open position.

Second, we are working to reduce unconscious bias. Our publicly available Managing Unconscious Bias class encourages our people to challenge and correct bias as soon as they see it—in others, and in themselves. We've also doubled down by adding two additional internal programs: Managing Inclusion, which trains managers to understand the issues that affect marginalized communities, and Be The Ally, which gives everyone the common language, tools, and space to practice supporting others.

Third, we have created Facebook University. We want to increase access and opportunity for students with an interest in software engineering, business, and analytics. Facebook University (FBU) gives underrepresented students extra training and mentorship earlier in their college education. We started FBU in 2013 with 30 students and expect to have 280 in 2018. More than 500 students have graduated

from this program, with many returning to Facebook for internships and full-time jobs.

Finally, we have many partnerships to move the numbers nationally such as Black Girls Code, All Star Code, Hack the Hood, The Hidden Genius Project, Level Playing Field Institute, Yes We Code, Streetcode Academy, Dev Color, Dev Bootcamp and Techbridge. And, we now recruit at 300 Universities—including historically black colleges and universities (HBCUs) like Spelman, Morehouse, Howard, NCA&T, and Morgan State (EIR) and the HBCU Faculty Summit.

We're committed to building a more diverse, inclusive Facebook. Much like our approach to launching new products on our platform, we are willing to experiment and listen to feedback.

Question 30. How are your entities working to address issues of discrimination, or lack of diversity, in your own workforce?

Answer. See Response to Question 29.

Question 31. Do you believe those efforts are sufficient and what do you believe is needed throughout the tech sector to address the mistreatment of some, and the need to expand ladders of opportunities for everyone?

Answer. See Response to Question 29.

Question 32. Like most companies, Facebook files numerous patents on its emerging technology and I'd like to raise concerns about some of the patents that your company has recently filed.

One is titled "Socioeconomic group classification based on user features" which is technology that would allow Facebook to group users into upper, middle, and working classes based on user action. It was recently discovered that Facebook has allowed advertisers to discriminate on the base of age.

How can we be confident that your company will crack down on discriminatory behavior as it is developing technology to group users into class?

Answer. Discriminatory advertising has no place on Facebook's platform and Facebook removes such content as soon as it becomes aware of it. Facebook's policies prohibit advertisers from discriminating against people on personal attributes such as race, ethnicity, color, national origin, religion, age, sex, sexual orientation, gender identity, family status, disability, and medical or genetic conditions. Facebook educates advertisers on our anti-discrimination policy, and in some cases, requires the advertisers to certify compliance with Facebook's anti-discrimination policy and anti-discrimination laws.

Facebook also uses machine learning to help identify ads that offer housing, employment, or credit opportunities. When an advertiser attempts to show an ad that Facebook identifies as offering a housing, employment, or credit opportunity and includes Facebook's multicultural advertising segments, Facebook will disapprove the ad. Facebook also requires advertisers to certify that they are complying with Facebook's updated anti-discrimination policy and anti-discrimination laws when the advertiser attempts to show a housing, employment, or credit opportunity and uses any other audience segment on Facebook.

Question 33. What other uses could this patent possibly have?

Answer. See Response to Question 1.

Question 34. Equal Pay Day: Mr. Zuckerberg, the date you appeared before was Equal Pay Day in America, which symbolizes the number of extra days a typical woman who works full-time, year-round must work into this year to be paid what a typical white man got paid. Women are still only paid 80 cents on the dollar compared to men. It's estimated that women employed full time in the U.S. will lose nearly $900 billion to the wage gap this year. I'm passionate about getting underrepresented folks into the job opportunities that our tech revolution provides, and equal pay goes along with creating those ladders of opportunities.

Is this an issue you are aware of and active on within your operations?

Answer. At Facebook, women and men receive equal pay for equal work and have done so for many years. This is an absolute minimum standard for a diverse business such as ours and we continually review our hiring and compensation practices to ensure this remains the case. Compensation at Facebook is made up of base salary, cash bonus or commission, and equity in the company. We work hard to avoid unconscious bias affecting how much people get paid. Managers don't make decisions about compensation increases—instead, we use a formulaic approach that determines pay based on performance and level.

Opportunities for advancement and leadership within the company are also crucial. For our women employees, we run a series of development workshops and training programs designed to provide a strong network of support, along with the tools they need to be the best leaders they can be across different levels in the company. We hold ourselves accountable because this matters to us. In 2017, the num-

ber of women employees globally rose from 33 percent to 35 percent and the number of women in technical roles increased from 17 percent to 19 percent. Between 2014 when we first publicly reported our representation data and 2017, the number of women in leadership roles has increased from 23 percent to 28 percent.

We are committed to increasing the representation of women at all levels. We know we're not where we need to be, and we're committed to making real progress.

With a global community of over two billion people on Facebook, greater diversity and inclusivity are critical to achieving our mission. Studies have shown that cognitive diversity on teams that are working on hard problems produces better results. Diversity helps us build better products, make better decisions, and better serve our community.

Question 35. Can you provide us confirmation, including figures, that your pay for women matches their male counterparts?

Answer. See Response to Question 32.

Question 36. And that you appropriately compensate all of your employees based on their job title and value to the company?

Answer. See Response to Question 32.

Question 37. Facebook's self-regulation of Campaign and Issue Ads & the Honest Ads Act: You recently announced that political ads run on Facebook are now going to be subject to heightened transparency requirements, such as including disclaimers stating who paid for the ad, and making it easier for viewers to see the ads that a page is running. I think this is a good first step but there are several questions I have regarding its implementation and how you will enforce this new policy.

What if you have an organization, let's call them "XYZ," who wants to post an issue or political ad, but they have never filed reports with the FEC, they are not registered with the IRS as a nonprofit, and they don't appear to have a website?

Answer. We now require more thorough documentation from advertisers who want to run ads with political content. Any person who wants to run one of these ads must upload an identification document and provide the last four digits of their Social Security number. They also must prove residency in the U.S. by providing a residential mailing address. Once they provide the address, we mail a letter with a code that the person must provide to us in order to become authorized to run ads with political content.

Question 38. You have said that advertisers running political ads and issue ads will have to be "authorized," and that Facebook will confirm their identity and location before running ads. What does it mean to "confirm their identity?"

Answer. See Response to Question 37.

Question 39. Walk me through how this ad would be treated under Facebook's new policies.

Answer. See Response to Question 37.

Question 40. So, this ad will say "paid for by XYZ." But there is no public record of XYZ, besides the fact that they have a Facebook page. Would you let a mysterious group like this run an ad on Facebook without any further information about who they are?

Answer. See Response to Question 37.

Question 41. Will you require any further verification from this group?

Answer. See Response to Question 37.

Question 42. Will these transparency measures you are discussing tell you who paid the Facebook page to run the ad? In other words, will Facebook disclose the sources of funding for these political ads?

Answer. Once verified as described above in response to Question 1, these advertisers will have to include a disclosure in these ads, which reads: "Paid for by." When users click on the disclosure, they will be able to see details about the advertiser. These ads will also all appear in a searchable archive, available at www.facebook.com/politicalcontentads, which includes information about how much the advertiser spent on the ad, how many people saw it, and general demographic information about the people who saw it.

Question 43. What if a foreign government gave money to a Facebook page with a U.S. address to run political ads? Would you tell that to viewers?

Answer. These are real challenges and reflect problems largely outside our control, but we will continue to work to improve our enforcement of ads that violate our policies.

Question 44. What if a foreign government gave money to a Facebook page through a series of shell companies or LLCs?

Answer. See Response to Question 43.

Question 45. How will Facebook know who the real donors to this group are?

Answer. See Response to Question 43.

Question 46. How is Facebook defining a "political ad" and an "issue ad" subject to these heightened transparency measures?

Answer. Our Political Advertising Policy (*https://www.facebook.com/policies/ads/restricted_content/political*) applies to any ad that:

- Is made by, on behalf of or about a current or former candidate for public office, a political party, a political action committee or advocates for the outcome of an election to public office;
- Relates to any election, referendum or ballot initiative, including "get out the vote" or election information campaigns;
- Relates to any national legislative issue of public importance in any place where the ad is being run; or
- Is regulated as political advertising.

We further define "national legislative issue of public importance" as including twenty issues. Ads that take a position on one or more of these issues are covered by the policy. To develop this initial list (which we expect to evolve over time), we worked with the non-partisan Project and many other stakeholders from across the political spectrum.

We determine whether an ad is subject to our Political Advertising policy based on the content of the ad.

Question 47. Is the "political ad/issue ad" determination based on the content of a particular ad, or the identity of the advertiser running the ad, or some other criteria?

Answer. See Response to Question 46.

Question 48. Facebook sells several types of ads, including sponsored ads that appear directly in a user's newsfeed, and smaller ads that appear on the right column. Studies show that a large volume of political ads from the 2016 election ran in the right column rather than in a user's newsfeed.

Will all types of ads sold by Facebook, including smaller ads, be subject to these heightened transparency measures?

Answer. Yes, all ads with political content will be subject to this policy.

Question 49. You mentioned that the disclaimers Facebook is going to implement will say which Facebook page paid for the ad. Will it tell you exactly what organization or individual is behind that page?

Answer. We require the advertiser to disclose who paid for an ad with political content—regardless of whether that is an individual or an organization.

Question 50. Rob Goldman, the Vice President of Ads at your company, indicated that you are working with the "third parties" to develop these parameters. Who are these "third parties?"

Answer. See Response to Question 47.

Question 51. Will these ad transparency measures also apply to state and local elections?

Answer. Our Political Advertising policy applies to all advertisers running ads with political content. The products we have launched (authorization, disclaimer, and archive) are available to all advertisers running ads with political content to users in the U.S.

Question 52. Will these same measures apply to other platforms owned by Facebook, like Instagram?

Answer. Yes, the measures will apply to ads with political content shown on Instagram.

Question 53. New Employees—Content Review: In your testimony, you note that Facebook plans to hire an additional 5,000 workers for its security and content review teams, for a total of 20,000 workers by the end of this year. But Facebook first announced the plan for a 20,000 person security team in late October of last year, in response to concerns about Russian interference in the election.

Given the additional revelations about the role of Cambridge Analytica and other third party apps in compromising the privacy and personal information of at least 87 million users, do you still believe 20,000 is the appropriate level of staffing for Facebook's security team?

Answer. Our effort to make our platform safer and more secure is a holistic one that involves a continual evaluation of our personnel, processes, and policies, and we make changes as appropriate.

We are doubling the size of our security and content review teams (from 10,000 to 20,000) over the course of this year. We currently have approximately 15,000 people working on these teams.

Of that 15,000, more than 7,500 people review content around the world.

- Our content review team is global and reviews reports in over 50 languages.
- Reports are reviewed 24 hours a day, 7 days a week and the vast majority of reports are reviewed within 24 hours.
- Our goal is always to have the right number of skilled people with the right language capabilities to ensure incoming reports are reviewed quickly and efficiently.
- We hire people with native language and other specialist skills according to the needs we see from incoming reports.
- The team also includes specialists in areas like child safety, hate speech and counter-terrorism, software engineers to develop review systems, quality control managers, policy specialists, legal specialists, and general reviewers.

We are also using machine learning to better detect and action on content and people that should not be using our platform.

For example, we incorporated learnings from interference in previous elections to better detect and stop false accounts from spreading misinformation in more recent elections.

We recently shared how we are using machine learning to prevent bad actors like terrorists or scammers from using our platform (*https://www.facebook.com/notes/facebook-security/introducing-new-machine-learning-techniques-to-help-stop-scams/10155213964780766/*).

We employ a mix of full-time employees, contractors and vendor partners to assist with content review and help us scale globally.

We partner with reputable vendors who are required to comply with specific obligations, ns for resiliency, support, transparency, and user privacy.

Question 54. Will these new security and content review workers be direct employees of Facebook, or do you plan to outsource this work to third party entities?

Answer. See Response to Question 53.

Question 55. If the security review work is outsourced, how will Facebook vet those contractors, subcontractors, and employees and where will those employees be located?

Answer. See Response to Question 53.

Question 56. And how can Facebook assure its users that there will be transparency and accountability for any future breaches of privacy if the company is outsourcing its security work?

Answer. See Response to Question 53.

Question 57. Future Facebook Technology: One of your recent patent is titled "Dynamic eye tracking calibration" and another is called "Techniques for emotion detection and content delivery". The patent for the eye tracking technology says that "the (eye) calibration process is performed automatically in the background while the user uses a device." The second patent would use a device's camera to monitor your emotions and "display content based upon a received emotion type."

How does Facebook plan to use this technology?

Answer. Like many companies, we apply for a wide variety of patents to protect our intellectual property. Right now we're not building technology to identify people with eye-tracking cameras. However, we're always exploring how new technologies and methods can improve our services, and eye-based identification is one way that we could potentially reduce consumer friction and add security for people when they log into Oculus or access Oculus content.

If we implement this technology in the future, we will absolutely do so with people's privacy in mind, just as we do with movement information (which we anonymize in our systems).

As we continue to develop new virtual reality products and services, we're committed to being transparent and open about the information that we collect and how we use it, as well as any ways that changes over time.

Question 58. Will users be fully aware that their eyes and emotions are being tracked?

Answer. See Response to Question 57.

Question 59. Is Facebook confident it has the proper data security in place to have this intimate level of data on users?

Answer. See Response to Question 57.

Question 60. Facebook has reportedly been developing an in-home digital assistant similar to products like Alexa, will this also be tracking this granular level of data?

Answer. See Response to Question 57.

Question 61. The second patent says that content will be delivered on a person's perceived emotion type. Couldn't this be potentially dangerous in amplifying hateful messages?

Answer. See Response to Question 57.

Question 62. If a person focuses on an image of say, a propaganda image of immigrants, will this technology deliver more of this content?

Answer. See Response to Question 57.

Question 63. China's Facebook Access: In July 2009, the Chinese government blocked Facebook in China. The precise reason for that action remains obscure, but it fits into an overall pattern. The Chinese government is unwilling to allow a social media platform—foreign or domestic—to operate in China unless it agrees to abide by Chinese law. First, a social media platform must agree to censor content and conversations in line with directives from China's information authorities. And second, businesses that collect data from Chinese individuals can only store that data in China where, presumably, it would be easier for the Chinese government to access, via legal means or otherwise. You've made no secret of your desire to see Facebook available once again in China.

Could you please reveal to the Committee whether you are willing to agree to either of these requirements?

Answer. Because Facebook has been blocked in China since 2009, we are not in a position to know exactly how the government would seek to apply its laws and regulations on content were we permitted to offer our service to Chinese users. Since 2013, Facebook has been a member of the Global Network Initiative (GNI), a multi-stakeholder digital rights initiative. As part of our membership, Facebook has committed to the freedom of expression and privacy standards set out in the GNI Principles—which are in turn based on the Universal Declaration of Human Rights and the United Nations Guiding Principles on Business and Human Rights—and we are independently assessed on our compliance with these standards on a biennial basis.

In keeping with these commitments, rigorous human rights due diligence and careful consideration of free expression and privacy implications would constitute important components of any decision on entering China. Facebook has been blocked in China since 2009, and no decisions have been made around the conditions under which any possible future service might be offered in China.

Question 64. And will Facebook pledge to guarantee its future Chinese users the same level of privacy protection it gives its users in the U.S. and the European Union?

Answer. Everyone in the world deserves good privacy protection.

Question 65. Consent Agreement: The FTC consent agreement with Facebook requires an independent, biennial audit of Facebook's privacy controls—when exactly have those audits been conducted, and what were the results?

Answer. To date, three independent privacy assessments prepared by PwC have been completed and submitted to the FTC: a 180-Day Assessment (dated April 16, 2013), a biennial privacy assessment covering the period between February 12, 2013 and February 11, 2015 (dated April 13, 2015), and a biennial privacy assessment covering the period between February 12, 2015 and February 11, 2017 (dated April 12, 2017). In each of these assessments, PwC determined that Facebook's privacy controls were operating with sufficient effectiveness to protect the privacy information covered under the FTC Consent Order.

Question 66. Did Facebook inform any of its auditors of the Cambridge Analytica data leak? Did any of Facebook's auditors know about the Cambridge Analytic data leak?

Answer. Facebook routinely undertakes internal and external reviews, including undergoing biennial assessments under Facebook's consent agreement with the Federal Trade Commission, which focus on the functioning of privacy controls that are part of Facebook's privacy program. As a part of the assessments, our independent assessors (PwC) have onsite access to our personnel and records, and we provide them with such access to information and personnel as they request in order to perform their work. PwC is also permitted to conduct a number of tests to determine whether the privacy controls in place under our privacy program—including controls relating to developer's access to information—are working properly. In its capacity as independent assessor, PwC evaluates the sufficiency of our controls through independent testing and requesting information that we provide to conduct that evalua-

tion. Their focus is on evaluating the operation and sufficiency of our controls, rather than specific incidents.

Kogan's violation of Facebook's Platform Policies was widely reported at the time Facebook learned about it, including reporting in *The Guardian* on December 11, 2015, which reported that Kogan and his company, GSR, may have passed information Kogan's app had obtained from Facebook users to SCL Elections Ltd. No data was transferred to Kogan's app unless it was authorized by the users who installed his app, so there was not a data leak from Facebook's systems. However, based on public reports and testimony, it appears that Kogan may have improperly transferred data to Cambridge Analytica in violation of our policies.

Question 67. Does Facebook choose which policies and procedures the auditors look at? Please explain in detail how these policies and procedures are chosen? Does the 3rd party auditor have any say on what policies and procedures are examined? Does the FTC have any input on how an audit is structured?

Answer. Facebook's privacy assessments are conducted pursuant to the July 27, 2012 Consent Order. They are conducted by an independent third-party professional (PwC) pursuant to the procedures and standards generally accepted in the profession and required by the FTC, as set forth in the Consent Order. Facebook incorporated GAPP principles in designing its privacy program and related controls, which are considered industry leading principles for protecting the privacy and security of personal information. Facebook provided the FTC with summaries of these controls and engaged extensively with the FTC regarding the structure of its privacy program. Facebook has submitted copies of each assessment to the FTC.

Question 68. Will Facebook commit to making the entirety of PwC audit submitted to the Federal Trade Commission in 2017 public? If not, please describe in detail why.

Answer. The privacy assessments conducted by PwC contain both Facebook's and PwC's sensitive business information that are confidential in order to prevent competitive harm and to ensure the integrity of Facebook's privacy program, including the steps that we take to protect people's information. We have furnished these reports to the FTC and are prepared to review the reports with regulators and lawmakers with appropriate assurances that confidential information or information that could be exploited to circumvent Facebook's privacy protections will not be disclosed publicly.

Question 69. During the negotiations with the FTC in 2011, were you asked by them to remove the capability to expose friends from having their data utilized without their direct permission?

Answer. We furnished extensive information to the FTC regarding the ability for users to port their Facebook data (including friends data that had been shared with them) with apps on Facebook's platform, as part of the FTC's investigation culminating in the July 27, 2012 Consent Order. The Consent Order memorializes the agreement between Facebook and did not require Facebook to turn off the ability for people to port friends data that had been shared with them on Facebook to apps they used. Facebook voluntarily changed this feature of Platform in 2014, however.

It is worth noting that in 2011, Facebook offered more control and protection over the availability of friends data to apps than any other digital platform at the time, including mobile app platforms, which generally permitted apps to access user data and their friends' data without consent or any control. By contrast, Facebook notified users of each category of data an app could access—including friends data—before the user consented to the app, and also provided all users with controls that would prevent their friends from sharing their data with apps on Facebook's platform.

Question 70. Hospital Data Sharing Project: It was reported by CNBC on April 5 that your company was in talks with top hospitals and other medical groups as recently as March 2018 about a proposal to share data you possess with the patients. As of now, the project is reportedly "on hiatus" so that Facebook can do a better job of protecting individuals' data.

Please provide us the specific privacy concerns Facebook has with compiling your users' data with medical data possessed by the hospitals?

Answer. The medical industry has long understood that there are general health benefits to having a close-knit circle of family and friends. But deeper research into this link is needed to help medical professionals develop specific treatment and intervention plans that take social connection into account. With this in mind, last year Facebook began discussions with leading medical institutions, including the American College of Cardiology and the Stanford University School of Medicine, to explore whether scientific research using fully-anonymized Facebook data could help the medical community advance our understanding in this area. This work has not

progressed past the planning phase, and we have not received, shared, or analyzed anyone's data.

In March, we decided that we should pause these discussions so we can focus on other important work, including doing a better job of protecting people's data and being clearer with them about how that data is used in our products and services.

Question 71. Would you share any internal documents that led Facebook to put this project on hiatus?

Answer. See Response to Question 70.

Question 72. Data Details & FB Messenger Data: Based on the FTC-Facebook consent order, your company collects a great deal of personal information on its users including—the location (*e.g.,* city or state), age, sex, birthday, "Interested in" responses (*i.e.,* whether a user is interested in men or women), Relationship Status, Likes and Interests, Education (*e.g.,* level of education, current enrollment in high school or college, affiliation with a particular college, and choice of major in college), and name of employer of individuals.

Do you collect any other specific information you have on individual Facebook users?

Answer. In response to your specific questions, depending on which Services a person uses, we collect different kinds of information from or about them. This is described in our Data Policy:

- *Things you and others do and provide.* Information and content you provide. We collect the content, communications and other information you provide when you use our Products, including when you sign up for an account, create or share content, and message or communicate with others. This can include information in or about the content you provide (like metadata), such as the location of a photo or the date a file was created. It can also include what you see through features we provide, such as our camera, so we can do things like suggest masks and filters that you might like, or give you tips on using camera formats. Our systems automatically process content and communications you and others provide to analyze context and what's in them for the purposes described below. Learn more about how you can control who can see the things you share.
  - *Data with special protections:* You can choose to provide information in your Facebook profile fields or Life Events about your religious views, political views, who you are "interested in," or your health. This and other information (such as racial or ethnic origin, philosophical beliefs or trade union membership) could be subject to special protections under the laws of your country.
- *Networks and connections.* We collect information about the people, Pages, accounts, hashtags, and groups you are connected to and how you interact with them across our Products, such as people you communicate with the most or groups you are part of. We also collect contact information if you choose to upload, sync or import it from a device (such as an address book or call log or SMS log history), which we use for things like helping you and others find people you may know and for the other purposes listed below.
- *Your usage.* We collect information about how you use our Products, such as the types of content you view or engage with; the features you use; the actions you take; the people or accounts you interact with; and the time, frequency and duration of your activities. For example, we log when you're using and have last used our Products, and what posts, videos and other content you view on our Products. We also collect information about how you use features like our camera.
- *Information about transactions made on our Products.* If you use our Products for purchases or other financial transactions (such as when you make a purchase in a game or make a donation), we collect information about the purchase or transaction. This includes payment information, such as your credit or debit card number and other card information; other account and authentication information; and billing, shipping and contact details.
- *Things others do and information they provide about you.* We also receive and analyze content, communications and information that other people provide when they use our Products. This can include information about you, such as when others share or comment on a photo of you, send a message to you, or upload, sync, or import your contact information.
- *Device Information.* As described below, we collect information from and about the computers, phones, connected TVs and other web-connected devices you use that integrate with our Products, and we combine this information across dif-

ferent devices you use. For example, we use information collected about your use of our Products on your phone to better personalize the content (including ads) or features you see when you use our Products on another device, such as your laptop or tablet, or to measure whether you took an action in response to an ad we showed you on your phone on a different device.

Information we obtain from these devices includes:

- *Device attributes:* information such as the operating system, hardware and software versions, battery level, signal strength, available storage space, browser type, app and file names and types, and plugins.
- *Device operations:* information about operations and behaviors performed on the device, such as whether a window is foregrounded or backgrounded, or mouse movements (which can help distinguish humans from bots).
- *Identifiers:* unique identifiers, device IDs, and other identifiers, such as from games, apps or accounts you use, and Family Device IDs (or other identifiers unique to Facebook Company Products associated with the same device or account).
- *Device signals:* Bluetooth signals, and information about nearby Wi-Fi access points, beacons, and cell towers.
- *Data from device settings:* information you allow us to receive through device settings you turn on, such as access to your GPS location, camera, or photos.
- *Network and connections:* information such as the name of your mobile operator or ISP, language, time zone, mobile phone number, IP address, connection speed and, in some cases, information about other devices that are nearby or on your network, so we can do things like help you stream a video from your phone to your TV.
- *Cookie data:* data from cookies stored on your device, including cookie IDs and settings. Learn more about how we use cookies in the Facebook Cookies Policy (available at *https://www.facebook.com/policies/cookies/*) and Instagram Cookies Policy (available at *https://www.instagram.com/legal/cookies/*).

- *Information from partners.* Advertisers, app developers, and publishers can send us information through Facebook Business Tools they use, including our social plug-ins (such as the Like button), Facebook Login, our APIs and SDKs, or the Facebook pixel. These partners provide information about your activities off Facebook—including information about your device, websites you visit, purchases you make, the ads you see, and how you use their services—whether or not you have a Facebook account or are logged into Facebook. For example, a game developer could use our API to tell us what games you play, or a business could tell us about a purchase you made in its store. We also receive information about your online and offline actions and purchases from third-party data providers who have the rights to provide us with your information. Partners receive your data when you visit or use their services or through third parties they work with. We require each of these partners to have lawful rights to collect, use, and share your data before providing any data to us.

Question 73. Are you tracking and collecting information and data from within your messenger chat tool? If so, what specific data are you collecting?

Answer. See Response to Question 72.

Question 74. What about your other platforms, like Instagram, what type of data are you tracking there?

Answer. Our Instagram Data Policy describes the data we collect and is available at *https://help.instagram.com/519522125107875.*

Question 75. Are you preserving broad and full conversations?

Answer. See Response to Question 72 and 74.

Question 76. Is that something you would have available to provide law enforcement?

Answer. We reach out to law enforcement if we learn of content that we believe reflects a credible threat of imminent harm. We have been able to provide support to authorities around the world that are responding to the threat of terrorism, including in cases where law enforcement has been able to disrupt attacks and prevent harm. Further, as part of official investigations, government officials sometimes request data about people who use Facebook. We have strict processes in place to handle these government requests, and we disclose account records in accordance with our terms of service and applicable law. We publish more information on the standards that govern our release of information to law enforcement in our Law Enforcement Guidelines at *https://www.facebook.com/safety/groups/law/*

guidelines/, and release statistics on the frequency with which we receive and comply with law enforcement requests at *https://transparency.facebook.com/*.

Question 77. Data Protection on Facebook: Has Facebook ever launched a feature that had to be turned off because of the privacy implications?

Answer. Protecting people's information is at the heart of everything we do, and as our CEO has recently stated, we are serious about doing what it takes to protect our community. We have developed extensive systems and processes that are designed to protect our data and user data, to prevent data loss, to disable undesirable accounts and activities on our platform, and to prevent or detect security breaches. In addition to comprehensive privacy reviews, we put products through rigorous data security testing. We also meet with regulators, legislators, and privacy experts around the world to get input on our data practices and policies.

At Facebook, we make decisions about privacy through a cross-functional, cross-disciplinary effort that involves participants from departments across the company. This process is a collaborative approach to privacy that seeks to promote strong privacy protections and sound decision making at every stage of the product development process. Our privacy program is responsible for reviewing product launches, major changes, and privacy-related bug fixes to products and features to ensure that privacy policies and procedures are consistently applied and that key privacy decisions are implemented for the product. This approach has several key benefits.

- First, it is designed to consider privacy early in the product development process. This allows us to consider the benefits that a feature is intended to have for people who use our services, how data will be used to deliver those benefits, and how we can build features from the ground up that include privacy protections to enable those benefits while protecting people's information and putting them in control.
- Second, while complying with our obligations is critically important, taking a cross-disciplinary approach to privacy encourages us to think about data protection as more than just a compliance exercise. Instead, we evaluate how to design privacy into the features that we build, and consider this from the perspective of things like how we design interfaces that make data use intuitive, taking a consistent approach to privacy across our services, and building protections in how our software is engineered. Accordingly, while we scale our privacy review process depending on the complexity of a particular data use, reviews typically involve experts who evaluate proposed data practices from the perspective of multiple disciplines.

As part of our consent agreement with the Federal Trade Commission, we submit a report to the FTC every two years. That report is based on assessments conducted by an independent third party on a biennial basis, which require us to submit evidence to demonstrate the effectiveness of the program.

Question 78. If so, how many times has that happened, and how many users were impacted?

Answer. See Response to Question 77.

Question 79. Did you notify the users who were impacted?

Answer. See Response to Question 78.

Question 80. Facebook tracking software: How many websites have Facebook tracking software on them?

Answer. Facebook does not publish tracking software. When people visit apps or websites that feature our technologies—like the Facebook Like or Comment button—our servers automatically log (i) standard browser or app records of the fact that a particular device or user visited the website or app (this connection to Facebook's servers occurs automatically when a person visits a website or app that contains our technologies, such as a Like button, and is an inherent function of Internet design); and (ii) any additional information the publisher of the app or website chooses to share with Facebook about the person's activities on that site (such as the fact that a purchase was made on the site). This is a standard feature of the Internet, and most websites and apps share this same information with multiple different third-parties whenever people visit their website or app. For example, the Senate Commerce Committee's website shares information with Google and its affiliate DoubleClick and with the analytics company Webtrends. This means that, when a person visits the Committee's website, it sends browser information about their visit to each one of those third parties. More information about how this works is available at *https://newsroom.fb.com/news/2018/04/data-off-facebook/*.

During the week prior to April 16, 2018, on sites that use Facebook services, the Like button appeared on 8.4 million websites, the Share button on 931,000 websites

covering 275 million webpages, and there were 2.2 million Facebook pixels installed on websites.

Question 81. What percentage of all Internet sites have Facebook tracking software?

Answer. See Response to Question 80.

Question 82. Do you track users even when they are logged out from Facebook?

Answer. When people visit apps or websites that feature our technologies—like the Facebook Like or Comment button—our servers automatically log (i) standard browser or app records of the fact that a particular device or user visited the website or app (this connection to Facebook's servers occurs automatically when a person visits a website or app that contains our technologies, such as a Like button, and is an inherent function of Internet design); and (ii) any additional information the publisher of the app or website chooses to share with Facebook about the person's activities on that site (such as the fact that a purchase was made on the site). (See *https://www.facebook.com/policies/cookies*). This is a standard feature of the Internet, and most websites and apps share this same information with multiple different third-parties whenever people visit their website or app. For example, the Senate Commerce Committee's website shares information with Google and its affiliate DoubleClick and with the analytics company Webtrends. This means that, when a person visits the Committee's website, it sends browser information about their visit to each one of those third parties. More information about how this works is available at *https://newsroom.fb.com/news/2018/04/data-off-facebook/*.

When the person visiting a website featuring Facebook's tools is not a registered Facebook user, Facebook does not have information identifying that individual, and it does not create profiles for this individual.

We use the browser and app logs that apps and websites send to us in the following ways for non-Facebook users. First, these logs are critical to protecting the security of Facebook and to detecting or preventing fake account access. For example, if a browser has visited hundreds of sites in the last five minutes, that's a sign the device might be a bot, which would be an important signal of a potentially inauthentic account if that browser then attempted to register for an account. Second, we aggregate those logs to provide summaries and insights to websites and apps about how many people visit or use their product, or use specific features like our Like button—but without providing any information about a specific person. We do not create profiles for non-Facebook users, nor do we use browser and app logs for non-Facebook users to show targeted ads from our advertisers to them or otherwise seek to personalize the content they see. However, we may take the opportunity to show a general ad that is unrelated to the attributes of the person or an ad encouraging the non-user to sign up for Facebook.

When the individual is a Facebook user, we are also able to use this information to personalize their experiences on Facebook, whether or not they are logged out, but we will not target ads to users relying on this information unless the user allows this in their privacy settings.

We do not sell or share this information with third parties.

Question 83. Do you collect data on people who have chosen not to use Facebook?

Answer. See Response to Question 82.

Question 84. How is this data used?

Answer. See Response to Question 83.

Question 85. Does it inform a user's "interests" on Facebook?

Answer. See Response to Question 83.

Question 86. If it does inform a user's "interests", was any of the data collected passively from users while they were browsing sites outside of Facebook passed to Cambridge Analytica?

Answer. No. Kogan's app did not have access to advertising interests data or browser logs.

Question 87. When the option or opportunity was previously available for folks to get the user data of individuals' friends, what was the total pool of data points one could obtain of friends, or was it all the exact same?

Answer. In April 2014, we announced that we would more tightly restrict our platform APIs to prevent abuse. At that time we made clear that existing apps would have a year to transition—at which point they would be forced (1) to migrate to the more restricted API and (2) be subject to Facebook's new review and approval protocols. A small number of developers asked for and were granted short-term extensions beyond the one-year transition period, the longest of which lasted several months. These extensions ended several years ago. A transition period of this kind is standard when platforms implement significant changes to their technology base

and was necessary here to avoid disrupting the experience of millions of people. New apps that launched after April 30, 2014 were required to use our more restrictive platform APIs, which incorporated several key new elements, including:

- Institution of a review and approval process, called App Review (also called Login Review), for any app seeking to operate on the new platform that would request access to data beyond the user's own public profile, e-mail address, and a list of friends of the user who had installed and authorized the same app;
- Generally preventing new apps on the new platform from accessing friends data without review; and
- Providing users with even more granular controls over their permissions as to what categories of their data an app operating on the new platform could access.

Our investigation is ongoing and as part of it we are taking a close look at applications that had access to friends data under Graph API v.1.0 before we made technical changes to our platform to change this access.

Question 88. Why did you change the policy of getting access to friends back in 2015?

Answer. See Response to Question 87.

Question 89. Quality Assurance—Policy changes within the company: What kind of privacy review is required to make a change to the Facebook platform?

Answer. See Response to Question 77.

Question 90. Is this review of platform changes mandatory? If so, when did that level of review become mandatory?

Answer. See Response to Question 77.

Question 91. Before that level of review was required, what checks were in place to ensure that new features wouldn't adversely impact users' privacy?

Answer. See Response to Question 77.

Question 92. What level of employee seniority was required of employees to approve a launch of such a privacy-impacting feature? For example, have you ever let an intern make changes that impact people's privacy?

Answer. See Response to Question 77.

Question 93. The Cambridge Analytica Data: Given the confessions made in undercover clips, and the means by which Cambridge Analytica obtained and used Facebook data, would you ever allow them broad access to your platform's user data again?

Answer. No. Facebook banned Cambridge Analytica from our service. We understand that the company is now defunct.

Question 94. Do you believe they have violated the Federal Trade Commission Act and its broad prohibition against "unfair and deceptive acts and practices" by misrepresenting the terms of their Facebook app?

Answer. Facebook has not violated the Federal Trade Commission Act. Facebook is not in a position to determine whether third-party app developers violated the Act and leaves that determination to the FTC, although we can confirm that misrepresenting the terms of an app to users is a violation of Facebook's developer policies.

Question 95. Previously, would you request an app developer or academic researcher outline any contractual or other association with outside entities—such as foreign nationals or states, or other potentially dangerous private operations? Are you doing so now?

Answer. In November 2013, when Kogan's app first became active on the platform, apps generally could be launched on the Facebook Platform without affirmative review or approval by Facebook. Kogan's app used the Facebook Login service, which allowed users to utilize their Facebook credentials to authenticate themselves to third-party services. Facebook Login and Facebook's Graph API also allowed Kogan's app to request permission from its users to access certain categories of data that users had entered into their Facebook profiles, as well as certain data their friends had shared with them, if enabled by these friends' privacy settings.

The App Review process introduced in 2014 requires developers who create an app that asks for more than certain basic user information from installers to justify the data they are looking to collect and how they are going to use it. Facebook then reviews whether the developer has a legitimate need for the data in light of how the app functions. Only if approved following such review can the app ask for users' permission to get their data. Facebook has rejected more than half of the apps submitted for App Review between April 2014 and April 2018.

We are in the process of investigating every app that had access to a large amount of information before we changed our Platform in 2014. Where we have concerns, we will conduct interviews, make requests for information (RFI)—which ask a series of detailed questions about the app and the data it has access to—and perform audits that may include on-site inspections. If we determine that there has been improper use of data, we will ban those developers and notify everyone affected. Facebook is launching the Data Abuse Bounty to reward people who report any misuse of data by app developers. The Data Abuse Bounty, inspired by the existing bug bounty program that we use to uncover and address security issues, will help us identify violations of our policies.

Further, Facebook's Platform Policy makes clear to app developers the relevant requirements regarding users' privacy that apply to apps operating on the Platform, including the requirements to give users choice and control, and to respect user privacy. Application developers explicitly agree to Facebook's Statement of Rights and Responsibilities and Platform Policy when they set up their Facebook accounts. The Platform Policy imposes a variety of obligations on app developers regarding the features, functionality, data collection and usage, and content for apps on the Platform, as well as Facebook's right to take enforcement action if an application violates the Platform Policy.

Prior to the introduction of App review in 2014, the Facebook Platform Policy, included provisions to the following effect:

- *Give People Control: Section 2(8):* Delete all of a person's data you have received from us (including friend data) if that person asks you to . . .
- *Protect Data: Section 3(3):* Only use friend data (including friends list) in the person's experience in your app.
- *Protect Data: Section 3(10):* Don't transfer any data you receive from us (including anonymous, aggregate, or derived data) to any ad network, data broker or other advertising or monetization-related service.
- *Login: Section 7(4):* Request only the data and publishing permission your app needs.

The Platform Policy also outlined the actions Facebook could take for violations of the policy:

- *Things You Should Know: Section 6(8):* We can audit your app to ensure it is safe and does not violate our terms. If requested, you must provide us with proof that your app complies with our terms.
- *Things You Should Know: Section 6(15):* We may enforce against your app or website if we conclude that your app violated our terms or is negatively impacting the Platform. We may or may not notify you in advance.
- *Things You Should Know: Section 6(16):* Enforcement is both automated and manual, and can include disabling your app, restricting you and your app's access to Platform functionality, requiring that you delete data, terminating agreements with you or any other action we deem appropriate.

Question 96. Do you know exactly how much Kogan profited from the data he provided to Cambridge Analytica and any other entities?

Answer. GSR certified to Facebook that it received payments totaling approximately 750,000 GBP from SCL for services relating to Kogan's modeling and use of data gathered by his app. The certification also stated that Kogan used the proceeds to operate GSR. Recently, Kogan has stated publicly that the above payment came from SCL. Kogan has also recently testified to the UK Parliament that GSR received additional payments not reflected in his certification to 1Facebook.

Question 97. From your understanding, was Kogan on payroll with Cambridge Analytica when he ran the personality app on Facebook?

Answer. Kogan has testified that he was not on Cambridge Analytica's payroll when he shared data and provided services to Cambridge Analytica. Rather, Kogan testified that he owned GSR, which entered into an agreement with Cambridge Analytica to provide it with services relating to certain Facebook data.

Question 98. Did Facebook make any attempt to pro-actively contact the 87 million users you say had their data harvested by Cambridge Analytica in the more than two years after you were alerted to the breach? If not, why not?

Answer. When Facebook learned about Kogan's breach of Facebook's data use policies in December 2015, we took immediate action. We retained an outside firm to assist in investigating Kogan's actions, to demand that Kogan and each party he had shared data with delete the data and any derivatives of the data, and to obtain certifications that they had done so. Because Kogan's app could no longer collect

most categories of data due to changes in Facebook's platform, the company's highest priority at that time was ensuring deletion of the data that Kogan may have accessed before these changes took place. With the benefit of hindsight, we wish we had notified people whose information may have been impacted. Facebook has since notified all people potentially impacted with a detailed notice at the top of their News Feed.

Question 99. Why did Facebook hire Joseph Chancellor, who was the business partner of Aleksandr Kogan, around the same time as the Guardian article alerted you to the violation of your policies?

Answer. Mr. Chancellor is a quantitative researcher on the User Experience Research team at Facebook, whose work focuses on aspects of virtual reality. We are investigating Mr. Chancellor's prior work with Kogan through counsel.

Question 100. Why do you continue to employ him to this day?

Answer. See Response to Question 99.

Question 101. Did any of the Facebook employees who were embedded with the Trump presidential campaign have any sense that they were helping target ads with data that was obtained through these disreputable means?

Answer. While our investigation is ongoing, our review indicates that Facebook employees did not identify any issues involving the improper use of Facebook data in the course of their interactions with Cambridge Analytica during the 2016 U.S. Presidential campaign. No one from Facebook was assigned full time to the Trump campaign.

Question 102. Is there no way any red flags would have arisen from how either good the targeting data was, or the way they were using it?

Answer. We expect that advertisers will use targeted advertising, and many political campaigns use custom audiences. The fact that a campaign used a custom audience and the performance of that audience would not normally be an indicator of any wrongdoing.

Question 103. To your knowledge, what foreign actors or entities may have accessed the same level of data that Cambridge Analytica has utilized?

Answer. Kogan represented that, in addition to providing data to his Prosociality and Well-Being Laboratory at the University of Cambridge for the purposes of research, GSR provided some Facebook data to SCL Elections Ltd., Eunoia Technologies, and the Toronto Laboratory for Social Neuroscience at the University of Toronto. Our investigation is ongoing.

Question 104. Russia: Facebook has downplayed the reach of Russian advertising during the 2016 election.

But the company's main business model is based on giving ads and posts prominence in the feeds of well-targeted users.

Has Facebook performed any analyses that looks at smaller groups of people and how effective those ads were against targeted groups? If so, can Facebook share that information?

Answer. We learned from press accounts and statements by congressional leaders that Russian actors might have tried to interfere in the 2016 election by exploiting Facebook's ad tools. This is not something we had seen before, and so we started an investigation. We found that fake accounts associated with the IRA spent approximately $100,000 on around 3,500 Facebook and Instagram ads between June 2015 and August 2017. Our analysis also showed that these accounts used these ads to promote the roughly 120 Facebook Pages they had set up, which in turn posted more than 80,000 pieces of content between January 2015 and August 2017. The Facebook accounts that appeared tied to the IRA violated our policies because they came from a set of coordinated, inauthentic accounts. We shut these accounts down and began trying to understand how they misused our platform. We shared the ads we discovered with Congress, in a manner that is consistent with our obligations to protect user information, to help government authorities complete the vitally important work of assessing what happened in the 2016 election.

Question 105. Do your company's records show that Russia-backed ads and posts reached a higher number of people in certain states or regions of the United States?

Answer. Approximately 25 percent of the ads that we've identified and turned over to the Committee were geographically targeted to a region smaller than the United States. The ads (along with the targeting information) are publicly available at *https://democratsintelligence.house.gov/facebook-ads/social-media-advertisements.htm.*

Question 106. If so, how responsive were Facebook users in those targeted regions to the Russian posts and ads?

Answer. Below is an overview of our analysis to date of the IRA's ads:

- Impressions (an "impression" is how we count the number of times something is on screen, for example this can be the number of times something was on screen in a person's News Feed)
  - 44 percent of total ad impressions were before the U.S. election on November 8, 2016.
  - 56 percent of total ad impressions were after the election
- Reach (the number of people who saw a story at least once):
  - We estimate 11.4 million people in the U.S. saw at least one of these ads between 2015 and 2017.
- Ads with zero impressions:
  - Roughly 25 percent of the ads were never shown to anyone. That's because advertising auctions are designed so that ads reach people based on relevance, and certain ads may not reach anyone as a result.
- Amount spent on ads:
  - For 50 percent of the ads, less than $3 was spent.
  - For 99 percent of the ads, less than $1,000 was spent.
  - Many of the ads were paid for in Russian currency, though currency alone is a weak signal for suspicious activity.
- Content of ads:
  - Most of the ads appear to focus on divisive social and political messages across the ideological spectrum, touching on topics from LGBT matters to race issues to immigration to gun rights.
  - A number of the ads encourage people to follow Pages on these issues, which in turn produced posts on similarly charged subjects.

We estimate that roughly 29 million people were served content in their News Feeds directly from the IRA's 80,000 posts over the two years. Posts from these Pages were also shared, liked, and followed by people on Facebook, and, as a result, three times more people may have been exposed to a story that originated from the Russian operation. Our best estimate is that approximately 126 million people may have been served content from a Page associated with the IRA at some point during the two-year period. This equals about four-thousandths of one percent (0.004 percent) of content in News Feed, or approximately 1 out of 23,000 pieces of content. While our data on Instagram is less complete, we believe another 16 million saw the IRA's Instagram posts starting in October 2016. Prior to that time, when our data is less incomplete, we believe another 4 million people may have seen this content.

Question 107. When did anyone at Facebook become aware that Russians or other foreign nationals were running ads in connection with the election?

Answer. See Response to Question 104.

Question 108. What happened with that information and what was done?

Answer. See Response to Question 104.

Question 109. FEC: Has anyone raised or approached you about potential infractions of any election laws that obtaining or using Facebook's data might be linked to including Cambridge Analytica's use of Facebook data?

Answer. We have a compliance team that trains our sales representatives to comply with all Federal election law requirements in this area. We also have processes designed to identify inauthentic and suspicious activity and we also maintain a sanctions compliance program to screen advertisers and paid app developers. Facebook's denied party screening protocol involves checking paid app developers and advertisers against applicable denied party listings. Those screened remain in an on-going monitoring portfolio and are screened against changes to applicable denied party listings. Moreover, our payments subsidiaries file Suspicious Activity Reports on developers of certain apps as appropriate. However, like other offline and online companies, Facebook has limited insight into the use of shell corporations or other sophisticated structures that may disguise the true buyer. In addition, the general challenge of attributing online activities to specific governments or organizations is widely recognized in the intelligence and law enforcement communities.

Question 110. We are now learning that there is reason to believe that Cambridge Analytica and its foreign national employees participated in the decision making of its U.S. political committee clients, possibly in violation of our campaign finance

law.[9] What steps will you take to determine whether the companies behind political or issue ads posted on Facebook are not in violation of our campaign finance laws?

Answer. See Response to Question 109.

Question 111. Will you undergo this examination before these ads are allowed to be posted on your platform?

Answer. See Response to Question 109.

Question 112. Technological Capabilities or Limitations to Protecting Data: Is it fair to say that not only were you not vigilant in following up or tracking those who have assessed Facebook's data, but that you have no technical solutions to track data activity once it's outside your network, such as specialty whether it's properly deleted?

Answer. We use a variety of tools to enforce Facebook policies against violating parties, including developers. We review tens of thousands of apps per year and regularly disapprove noncompliant apps as part of our proactive review process. We also use tools like cease and desist letters, account suspensions, letter agreements, and civil litigation. For example, since 2006, Facebook has sent over 1,150 cease-and-desist letters to over 1,600 targets. In 2017, we took action against about 370,000 apps, ranging from imposing certain restrictions to removal of the app from the platform. Moreover, we have required parties who have procured our data without authorization to delete that data. We have invested significant resources in these efforts. Facebook is presently investigating apps that had access to large amounts of information before we changed our platform policies in 2014 to significantly reduce the data apps could access. To date, around 200 apps (from a handful of developers: Kogan, AIQ, Cube You, the Cambridge Psychometrics Center, and myPersonality) have been suspended pending a thorough investigation into whether they did in fact misuse any data.

Question 113. Or at least without a formal deep audit?

Answer. See Response to Question 112.

Question 114. What are the specific aspects of a formal audit, including the technical capabilities?

Answer. With respect to our audit of all apps that had access to large amounts of information before we changed our platform policies in 2014, where we have concerns that data may have been shared outside the app in violation of our policies, we will conduct interviews, make requests for information (RFI)—which ask a series of detailed questions about the app and the data it has access to—and perform audits that may include on-site inspections.

Question 115. And still with an audit, can you clarify what level of detail you have or could find misuse from someone?

Answer. See Response to Question 114.

Question 116. It's being reported, and opined by others in your field, including former employees of yours, that it's notoriously difficult to track down and secure personal information once it has been unleashed.

So that makes it all the more important to be vigilant on the front end, no?

Answer. In April 2014, we announced that we would more tightly restrict our platform APIs to prevent abuse. At that time we made clear that existing apps would have a year to transition—at which point they would be forced (1) to migrate to the more restricted API and (2) be subject to Facebook's new review and approval protocols. A small number of developers asked for and were granted short-term extensions beyond the one-year transition period, the longest of which lasted several months. These extensions ended several years ago. A transition period of this kind is standard when platforms implement significant changes to their technology base and was necessary here to avoid disrupting the experience of millions of people. New apps that launched after April 30, 2014 were required to use our more restrictive platform APIs. We required apps seeking additional categories of data to undergo proactive review by our internal teams. We rejected more than half of the apps seeking these permissions, including the second version of Kogan's app.

We review apps to ensure that the requested permissions clearly improve the user experience and that the data obtained is tied to an experience within the app. We conduct a variety of manual and automated checks of applications on the platform for Policy compliance, as well as random sampling. When we find evidence of or receive allegations of violations, we investigate and, where appropriate, employ a number of measures, including restricting applications from our platform, preventing developers from building on our platform in the future, and taking legal action where appropriate.

---

[9] *http://fortune.com/2018/03/26/watchdog-alleges-cambridge-analytica-violated-election-law/*

Recently, we announced a number of additional steps we're taking to address concerns raised by Kogan's app.

- *Review our platform.* We will investigate all apps that had access to large amounts of data before the platform changes we announced in 2014, and we will audit any app where we identify suspicious activity. If we identify misuses of data, we'll take immediate action, including banning the app from our platform and pursuing legal action if appropriate.
- *Tell people about data misuse.* We will tell people about apps that have misused their data. This includes building a way for people to know if their data might have been accessed via the app. Moving forward, if we remove an app for misusing data, we will tell everyone who used it.
- *Turn off access for unused apps.* If someone has not used an app within the last three months, we will turn off the app's access to their data.
- *Restrict Facebook Login data.* We are changing Login, so that the only data that an app can request without app review will include name, profile photo, and e-mail address. Requesting any other data will require approval from Facebook. We will also no longer allow apps to ask for access to information like religious or political views, relationship status and details, custom friends lists, education and work history, fitness activity, book reading and music listening activity, news reading, video watch activity, and games activity. We will encourage people to manage the apps they use. We already show people what apps their accounts are connected to and allow them to control what data they've permitted those apps to use. But we're making it easier for people to see what apps they use and the information they have shared with those apps.
- *Reward people who find vulnerabilities.* We launched the Data Abuse Bounty program so that people can report to us any misuses of data by app developers.
- *Update our policies.* We have updated our terms and Data Policy to explain how we use data and how data is shared with app developers.

Question 117. How much do you anticipate Facebook will be investing in your investigations or audits into app developers, and others who have had access to user data?

How much value would you estimate that Facebook has lost through this latest string of controversies, and the Cambridge Analytica data security issue?

Answer. We are investing so much in security that our costs will increase significantly. But we want to be clear about what our priority is: protecting our community is more important than maximizing our profits.

Question 118. And how much personally to do suspect you've lost?

Answer. See Response to Question 117.

Question 119. What personal data of yours, or say your wife's, is available or exploitable on any of the platforms you run?

Answer. Mark Zuckerberg's data was among the data that was shared with Kogan's app, which may have been improperly shared with Cambridge Analytica.

Question 120. Seems like millions, or even billions, spent earlier and being proactively protective would, or could have, saved tens of billions overall, wouldn't you agree?

Answer. See Response to Question 116.

Question 121. Do you think there's enough accountability at all levels within Facebook, including for yourself, Ms. Sandberg, others in senior positions?

Answer. As our CEO Mark Zuckerberg has said, when you are building something unprecedented like Facebook, there are going to be mistakes. What people should hold us accountable for is learning from the mistakes and continually doing better—and, at the end of the day, making sure that we're building things that people like and that make their lives better.

Question 122. The *Washington Post* has reported that Mr. Kogan says that none of the data that was taken for research purposes in 2013 was provided to Cambridge Analytica. He says that after he began working with Cambridge Analytica, he sent out a new survey to Facebook users, with new terms of service that allowed for broad uses of the data. That new survey app collected data from nearly 300,000 Facebook users and captured data on 30 million of their friends. He says he has deleted all the data that he obtained from Facebook.

Can Facebook prove all of this as fact or fiction?

Answer. On December 11, 2015, *The Guardian* published an article reporting that Kogan and his company, GSR, may have passed information his app had obtained from Facebook users to SCL Elections Ltd. (SCL)/Cambridge Analytica. By doing so,

Kogan and his company violated Facebook's Platform Policies, which explicitly prohibited selling or licensing user data accessed from Facebook and from sharing any user data accessed from Facebook with any ad network, data broker, or other advertising or monetization-related service. For this reason, Facebook immediately banned his app from our platform and launched an investigation into these allegations. Kogan signed a certification declaring that he had deleted all data that he obtained through his app and obtained certifications of deletion from others he had shared data with, including Cambridge Analytica. In March 2018, new allegations surfaced that Cambridge Analytica may not have deleted data as it had represented. Our investigation of these matters is ongoing.

Question 123. Facebook's Definition and Regulatory Positions: Do you believe you are an actual media entity now?

Answer. Facebook does not create or edit the content that users share on its Platform, although we do take steps to arrange, rank and distribute that content to those who are most likely to be interested in it, or to remove objectionable content from our service. These activities are protected functions under Communications Decency Act Section 230 and the First Amendment.

Question 124. Are you solely a tech company?

Answer. We are, first and foremost, a technology company. Facebook does not create or edit the content that our users published on our platform. While we seek to be a platform for a broad range of ideas, we do moderate content in good faith according to published community standards in order to keep users on the platform safe, reduce objectionable content, and to make sure users participate on the platform responsibly.

Question 125. When it comes to news posts and political advertising, why should Facebook get a regulatory exemption that traditional media doesn't get?

Answer. Facebook is committed to transparency for all ads, including ads with political content. Facebook believes that people should be able to easily understand why they are seeing ads, who paid for them, and what other ads those advertisers are running. As such, Facebook only allows authorized advertisers to run ads about elections or issues that are being debated across the country. In order to be authorized by Facebook, advertisers will need to confirm their identity and location. Furthermore, all political ads will include a disclosure in their election-related ads, which reads: "Paid for by," and when users click on this disclosure they will be able to see details about the advertiser. Users will also be able to see an explanation of why they saw the particular ad. This is similar to the disclosure included on political TV advertisements.

Question 126. Facebook with Law Enforcement: How wide is the use and specific collection of social media data with law enforcement, say in a given year? (FBI, CBP, ICE)

Answer. As part of official investigations, government officials sometimes request data about people who use Facebook. We have strict processes in place to handle these government requests, and we disclose account records in accordance with our terms of service and applicable law. We also have law enforcement response teams available around the clock to respond to emergency requests. As part of our ongoing effort to share information about the requests we have received from governments around the world, Facebook regularly produces a Transparency Report about government requests to Facebook.

Question 127. Have you seen an increase is such request under the current Administration?

Answer. See Response to Question 126.

Question 128. Or has there been a variation in the type or aggressiveness of these requests over the same time?

Answer. See Response to Question 126.

Question 129. Social Media Addiction: Obvious the social media revolution has brought in a number of addition issues into play that we in Congress need to consider, from platforms for terrorist organizations and hate groups, to censorship and online addiction. And that is something I wanted to inquire about.

I know it was raised by one member during your hearing, but do you fund any research on the issue of potential social media addiction, and if not, would you consider funding independent third-party research in this area?

Answer. Facebook employs social psychologists, social scientists, and sociologists, and collaborates with top scholars to better understand well-being. Facebook has also pledged $1 million towards research to better understand the relationship between media technologies, youth development and well-being. Facebook is teaming up with experts in the field to look at the impact of mobile technology and social

media on kids and teens, as well as how to better support them as they transition through different stages of life. Facebook is committed to bringing people together and supporting well-being through meaningful interactions on Facebook.

RESPONSE TO WRITTEN QUESTIONS SUBMITTED BY HON. CHUCK GRASSLEY TO MARK ZUCKERBERG

Question 1. Please provide a comprehensive list of all forms of content or data Facebook collects on Facebook users from the Facebook platform, whether it is content or data created by the user or not.

Answer. As explained in our Data Policy, we collect three basic categories of data about people:

(1) data about things people do and share (and who they connect with) on our services,

(2) data about the devices people use to access our services, and

(3) data we receive from partners, including the websites and apps that use our business tools.

As far as the amount of data we collect about people, the answer depends on the person. People who have only recently signed up for Facebook have usually shared only a few things—such as name, contact information, age and gender. Over time, as people use our products, we receive more data from them, and this data helps us provide more relevant content and services. That data will fall into the categories noted above, but the specific data we receive will, in large part, depend on how the person chooses to use Facebook. For example, some people use Facebook to share photos, so we receive and store photos for those people. Some people enjoy watching videos on Facebook; when they do, we receive information about the video they watched, and we can use that information to help show other videos in their News Feeds. Other people seldom or never watch videos, so we do not receive the same kind of information from them, and their News Feeds are likely to feature fewer videos.

The data we have about people also depends on how they have used our controls. For example, people who share photos can easily delete those photos. The same is true of any other kind of content that people post on our services. Through Facebook's Activity Log tool, people can also control the information about their engagement—*i.e.,* their likes, shares and comments—with other people's posts. The use of these controls of course affects the data we have about people.

We recently announced improvements to our Download Your Information tool, as well as a new feature that makes it easier for people to see the information that's in their account on Facebook. These recently-expanded tools for accessing information will allow people to see their data, delete it, and easily download and export it.

Question 2. Please provide a comprehensive list of all ways Facebook uses each form of content or data. Please provide as much detail as possible. For example, does Facebook ever use location information to tell a business that a consumer physically went to a store after seeing an ad?

Answer. See Response to Question 1.

Question 3. Does Facebook collect or purchase information about non-Facebook users? If so, what information is collected? How does Facebook acquire the information? What are all the ways Facebook uses the information? Please provide a comprehensive list of all forms of data Facebook collects on individuals, not collected from the Facebook website.

a. Can a person who does not have a Facebook account request deletion of any data? How?

b. If Facebook has utilized the information of a person who does not have an account in any way, such as building advertising profile, will deletion of the data ensure deletion from advertising profiles or any other products that the data was used to compile?

Answer. Facebook does not create profiles or track website visits for people without a Facebook account.

When people visit apps or websites that feature our technologies—like the Facebook Like or Comment button—our servers automatically log (i) standard browser or app records of the fact that a particular device or user visited the website or app (this connection to Facebook's servers occurs automatically when a person visits a website or app that contains our technologies, such as a Like button, and is an inherent function of Internet design); and (ii) any additional information

the publisher of the app or website chooses to share with Facebook about the person's activities on that site (such as the fact that a purchase was made on the site). This is a standard feature of the Internet, and most websites and apps share this same information with multiple different third parties whenever people visit their website or app. For example, the Senate Commerce Committee's website shares information with Google and its affiliate DoubleClick and with the analytics company Webtrends. This means that, when a person visits the Committee's website, it sends browser information about their visit to each one of those third parties. More information about how this works is available at *https://newsroom.fb.com/news/2018/04/data-off-facebook/*.

When the person visiting a website featuring Facebook's tools is not a registered Facebook user, Facebook does not have information identifying that individual, and it does not create profiles for this individual.

We use the browser and app logs that apps and websites send to us—described above—in the following ways for non-Facebook users. First, these logs are critical to protecting the security of Facebook and to detecting or preventing fake account access. For example, if a browser has visited hundreds of sites in the last five minutes, that's a sign the device might be a bot, which would be an important signal of a potentially inauthentic account if that browser then attempted to register for an account. Second, we aggregate those logs to provide summaries and insights to websites and apps about how many people visit or use their product, or use specific features like our Like button—but without providing any information about a specific person. We do not create profiles for non-Facebook users, nor do we use browser and app logs for non-Facebook users to show targeted ads from our advertisers to them or otherwise seek to personalize the content they see. However, we may take the opportunity to show a general ad that is unrelated to the attributes of the person or an ad encouraging the non-user to sign up for Facebook.

When the individual is a Facebook user, we are also able to use this information to personalize their experiences on Facebook, whether or not they are logged out, but we will not target ads to users relying on this information unless the user allows this in their privacy settings. We do not sell or share this information with third-parties.

Question 4. When a user deletes information from Facebook, is that information still used to inform advertising?

a. If it is, how does the user change this?

b. When a user deletes their Facebook account, is underlying data still used in any way, including to inform advertising profile? Can the user prevent any further use?

Answer. The audience with which someone chooses to share their information is independent of whether we use that information to personalize the ads and other content we show them. Specifically, our Data Policy explains that we may use any information that people share on Facebook "to deliver our Products, including to personalize features and content (including your News Feed, Instagram Feed, Instagram Stories and ads)." However, people can use our Ad Preferences tool to see the list of interests that we use to personalize their advertising. This means that, for example, a person who is interested in cars can continue to share that interest with their friends but tell us not to assign them an interest in ads for ad targeting purposes.

Likewise, the audience of a post does not determine whether a post is retained. Someone can choose to share a post with "Only Me" (meaning that they don't want anyone to see it but want to retain it in their Facebook account). They may also choose to delete the information entirely. When people choose to delete something they have shared on Facebook, we remove it from the site. In most cases, this information is permanently deleted from our servers; however, some things can only be deleted when a user permanently deletes their account.

Question 5. How long does Facebook keep a user's data after they delete their account? Is there any data that is not deleted from Facebook's servers?

Answer. In general, when a user deletes their account, we delete things they have posted, such as their photos and status updates, and they won't be able to recover that information later. (Information that others have shared about them isn't part of their account and won't be deleted.)

There are some limited exceptions to these policies: For instance, information can be accessed and preserved for an extended period when it is the subject of a legal request or obligation, governmental investigation, or investigations of possible violations of our terms or policies, or otherwise to prevent harm. We also retain information from accounts disabled for terms violations for at least a year to prevent repeat abuse or other term violations.

Question 6. In your testimony you stated that the user has complete control over their Facebook page.

a. Can a user make their profile invisible, so it cannot be found by searching Facebook or the web?

b. Can a user choose to make their name or picture private?

c. Can a user opt out of specific uses of their data, such as academic research?

Answer. When someone creates a profile on Facebook, the purpose of the profile is to enable others on Facebook to see whatever information the person chooses to add to his or her profile. However, people are in control of what information they add—only a person's name and limited other data is required to create a Facebook profile. And, for nearly all information that people choose to add to their profiles, they can choose who is eligible to see this information. For example, a person might choose to share his or her hometown only with his or her friends.

A limited amount of information that people provide—including their name and, if they choose to add one, their profile photo—is always public on Facebook. Among other things, this helps us inform a user before they make or accept a friend request of the identity of the person with whom he or she is about to connect.

Through Facebook's Settings, people can make a range of choices about how their information will be used, including instructing that they do not want search engines to link to their profiles. We inform people that, even if they choose not to be linked to in search engines, anyone may see information that they share if they set the audience for that information to Public.

Question 7. With regard to academic research, you recently updated your data policy as it was reported that Facebook was looking into partnering with healthcare providers to conduct medical research.

a. Why was it not disclosed earlier to users that their data could be used for research?

b. How does a user opt out of being a subject of medical or other academic research?

c. If they cannot, why not? Will you change this?

Answer. Facebook was exploring this type of data sharing because of the general health benefits to having a close-knit circle of family and friends and the need for more research on the impact of social connection on health. Deeper research into this link is needed to help medical professionals develop specific treatment and intervention plans that take social connection into account. With this in mind, last year Facebook began discussions with leading medical institutions, including the American College of Cardiology and the Stanford University School of Medicine, to explore whether scientific research using fully-anonymized Facebook data could help the medical community advance our understanding in this area. This work did not progress past the planning phase, and we have not received, shared, or analyzed anyone's data.

In March we decided that we should pause these discussions so we can focus on other important work, including doing a better job of protecting people's data and being clearer with them about how that data is used in our products and services.

Our Data Policy has explained that we have engaged in research collaborations for several years. As part of a general effort to be more transparent, we updated our Data Policy recently to provide additional detail on a range of practices, including academic research. We also explain this in other ways, including announcements in our Newsroom and in a dedicated website providing more information about research at Facebook.

Question 8. Does Facebook currently collect, or have any plans to collect, anonymized medical information of Americans?

a. If so, what are the planned or potential uses of this information?

Answer. See Response to Question 7.

Question 9. In your testimony you stated that it would be too long a webpage if you provide a list of all the ways data is used. Is there a reason you could not have a short, easy to understand list, and a long comprehensive list for those who are interested to learn more?

Answer. We believe that it's important to communicate with people about the information that we collect and how people can control it. This is why we work hard to provide this information to people in a variety of ways: in our Data Policy, and in Privacy Basics, which provides walkthroughs of the most common privacy questions we receive. Beyond simply disclosing our practices, we also think it's important to give people access to their own information, which we do through our Download Your Information and Access Your Information tools, Activity Log, and Ad Pref-

erences, all of which are accessible through our Privacy Shortcuts tool. We also provide information about these topics as people are using the Facebook service itself.

Facebook seeks, as much as possible, to put controls and information in context within its service. While "up front" information like that contained in the terms of service are useful, research overwhelmingly demonstrates that in-product controls and education are the most meaningful to people and the most likely to be read and understood. On-demand controls are also important, and we recently redesigned our entire settings menu on mobile devices from top to bottom to make things easier to find. We also created a new Privacy Shortcuts menu where users can control their data in just a few taps, with clearer explanations of how our controls work. The experience is now clearer, more visual, and easy-to-find.

Improving people's understanding of how digital services work is an industry-wide challenge that we are highly committed to addressing. That's why, over the last 18 months, we've run a global series of design workshops called "Design Jams," bringing together experts in design, privacy, law and computer science to work collaboratively on new and innovative approaches. These workshops have run in Paris, London, Dublin, Berlin, Sao Paolo, Hong Kong and other cities, and included global regulators and policymakers. At these workshops, expert teams use "people centric design" methods to create innovative new design prototypes and experiences to improve transparency and education in digital services. These workshops inform Facebook's constantly-improving approach.

In recognition of the need for improved approaches to data transparency across all digital services, working with partners from academia, design and industry we recently launched TTC Labs, a design innovation lab that seeks to improve user experiences around personal data. TTC Labs is an open platform for sharing and innovation and contains insights from leading experts in academia, design and law, in addition to prototype designs from the Design Jams, template services and open-source toolkits for people-centric design for transparency, trust and control of data. Working collaboratively, and based on open-source approaches, TTC Labs seeks to pioneer new and more people-centric best practices for people to understand how their data is used by digital services, in ways that they find easy to understand and control.

Facebook is highly committed to improving people's experience of its own services as well as investing in new innovations and approaches to support improvements across the industry.

Question 10. It has been reported that Facebook's download your information tool, contrary to your testimony, does not contain all the data Facebook has collected on that individual consumer. Can you explain that discrepancy? Will you be changing this?

Answer. Our Download Your Information or "DYI" tool is Facebook's data portability tool and was launched many years ago to let people access and download many types of information that we maintain about them. The data in DYI and in our Ads Preferences tool contain each of the interest categories that are used to show people ads, along with information about the advertisers currently running ads based on their use of an advertiser's website or app. People also can choose not to see ads from those advertisers. We recently announced expansions to Download Your Information, which, among other things, will make it easier for people to see their data, delete it, and easily download and export it. More information is available at *https://newsroom.fb.com/news/2018/04/new-privacy-protections/*.

Responding to feedback that we should do more to provide information about websites and apps that send us information when people use them, we also announced plans to build Clear History. This new feature will enable users to see the websites and apps that send us information when they use them, delete this information from their account, and turn off Facebook's ability to store it associated with their account going forward.

We have also introduced Access Your Information. This feature provides a new way for people to access and manage their information. Users can go here to delete anything from their timeline or profile that they no longer want on Facebook. They can also see their ad interests, as well as information about ads they've clicked on and advertisers who have provided us with information about them that influence the ads they see. From here, they can go to their ad settings to manage how this data is used to show them ads.

Question 11. Facebook has previously stated that private messages are not scanned for advertising, but are scanned for content such as child pornography and facilitating genocide. Is there any other way in which private messages are used by Facebook or any third party?

Answer. The way Facebook uses messages can be found in our Data Policy, located at: *https://www.facebook.com/policy.php*.

Question 12. When a user logs in to Facebook, does Facebook continue to track, through cookies or other trading tools, the users pages visited (a) while the user is still logged onto the Facebook page, and (b) after the user logs out of the Facebook page?

Answer. See Response to Question 3.

Question 13. Please provide a detailed explanation how Facebook tracks a user's Internet browsing activity. Where is this disclosed on the Facebook website and could it be disclosed more fully?

Answer. We do not use web browsing data to show ads to non-users or otherwise store profiles about non-users. Our goal is to show people content (including advertising) that is relevant to their interests. We use information people have provided on Facebook—such as things they've liked or posts they've engaged with—to help determine what people will be interested in. Like most online advertising companies, we also inform our judgments about what ads to show based on apps and websites that people use off of Facebook. People can completely turn off our use of web browser data and other data from third-party partners to show them ads through a control in Ads Preferences. They can also customize their advertising experience by removing interests that they do not want to inform the Facebook ads they see. In addition, a person's browser or device may offer settings that allow users to choose whether browser cookies are set and to delete them

Question 14. Can people opt-out of being tracked across the Web by Facebook via cookies and other tracking tools? How?

Answer. See Responses to Questions 10 and 13.

Question 15. Has Facebook been collecting call history and SMS data from Android phones? If yes, how has it been collected and what is Facebook doing with this information?

Answer. Call and text history logging is part of an opt-in feature that lets people import contact information to help them connect with people they know on Facebook and Messenger. We introduced the call and text history component this feature for Android users several years ago, and currently offer it in Messenger and Facebook Lite, a lightweight version of Facebook, on Android.

Contact importers are fairly common among social apps and services as a way to more easily find the people users want to connect with. They help users find and stay connected with the people they care about, and provide them with a better experience across Facebook.

Before we receive anyone's call and text history, they specifically grant us permission to access this data on their device and separately agree to use the feature. If, at any time, they no longer wish to use this feature, they can turn it off, and all previously shared call and text history shared via that app is deleted. People can also access information they previously imported through the Download Your Information tool.

Question 16. Does Facebook scan users' photos to generate biometric data on them? Does Facebook scan photos for any reason other than to match photos based on facial recognition and to search for inappropriate content?

Answer. Facebook uses facial recognition technology to provide people with products and features that enhance online experiences for Facebook users while giving them control over this technology. Facebook's facial recognition technology helps people tag their friends in photos; gives people an easier and faster way to privately share their photos with friends; helps people with visual impairments by generating descriptions of photos that people using screen readers can hear as they browse Facebook; lets people know when a photo or video of them has been uploaded to Facebook, even if they are not tagged; and helps prevent people from impersonating other Facebook users.

Facial recognition technology uses machine-learning algorithms to analyze the pixels in photos and videos in which a user is tagged, and the photo used by the person as his or her profile picture, and generates a unique number called a template. When a photo or video is uploaded to Facebook, Facebook uses the template to attempt to identify someone by determining whether there are any faces in that content, and analyzing the portion of the image in which the face appears to compare it against certain Facebook users depending on the purpose for which facial recognition is being performed.

Facebook has not shared and does not have plans to share or make available to any third party its facial recognition templates. Moreover, these templates do not provide meaningful information on their own; they can be used to identify a person

only in conjunction with Facebook's software. They could not be reverse-engineered to recreate someone's face.

Facebook designed its facial-recognition technology and the applications that use it with privacy considerations in mind and incorporated various safeguards and controls that protect both (1) users' ability to control the collection, use, and disclosure of their personal information, and (2) the security of that personal information.

Facebook gives users control over whether Facebook uses facial recognition to recognize them in photos and videos. That control is exercised through users' privacy settings. If a user chooses to turn facial recognition off, Facebook does not create a template for that person or deletes any template it has previously created. Facebook will then be unable to recognize that person in any photos or videos that are uploaded to the service. Facebook also deletes templates of people who delete their Facebook accounts. Additionally, Facebook does not maintain templates for users who have no photos tagged of themselves and do not have a profile photo that is capable of being used to generate a face signature or template (*e.g.,* where a user has no profile photo, where a user's profile photo does not contain a human face, or where a user's profile photo contains multiple untagged faces).

We inform people about our use of facial recognition technology through the Data Policy, Help Center, posts on Facebook, and direct user notifications. Facebook users are told that they can opt out of facial recognition at any time—in which case Facebook will delete their template and will no longer use facial recognition to identify them.

In creating facial recognition templates, Facebook uses only data that people have voluntarily provided to Facebook: the photos and videos that people have voluntarily uploaded to Facebook (including public profile pictures) and the tags people have applied to those photos and videos. Facebook does not use facial recognition to identify someone to a stranger.

Question 17. Does Facebook collect user data through cross-device tracking? What types of data are collected? If a user accesses their Facebook account through a mobile device, for example, what information does Facebook collect about that mobile device? And what access, if any, does Facebook have to other data located on that user's mobile device? What are all the ways in which Facebook uses this data?

Answer. Facebook's services inherently operate on a cross-device basis: understanding when people use our services across multiple devices helps us provide the same personalized experience wherever people use Facebook—for example, to ensure that a person's News Feed or profile contains the same content whether they access our services on their mobile phone or in a desktop computer's web browser.

In support of those and other purposes, we collect information from and about the computers, phones, connected TVs and other web-connected devices our users use that integrate with our Products, and we combine this information across a user's different devices. For example, we use information collected about a person's use of our Products on their phone to better personalize the content (including ads) or features they see when they use our Products on another device, such as their laptop or tablet, or to measure whether they took an action in response to an ad we showed them on their phone or on a different device.

Information we obtain from these devices includes:

- *Device attributes.* Information such as the operating system, hardware and software versions, battery level, signal strength, available storage space, browser type, app and file names and types, and plugins.
- *Device operations.* Information about operations and behaviors performed on the device, such as whether a window is foregrounded or backgrounded, or mouse movements (which can help distinguish humans from bots).
- *Identifiers.* Unique identifiers, device IDs, and other identifiers, such as from games, apps or accounts people use, and Family Device IDs (or other identifiers unique to Facebook Company Products associated with the same device or account).
- *Device signals.* Bluetooth signals, and information about nearby Wi-Fi access points, beacons, and cell towers.
- *Data from device settings.* Information a user allows us to receive through device settings they turn on, such as access to their GPS location, camera, or photos.
- *Network and connections.* Information such as the name of a user's mobile operator or ISP, language, time zone, mobile phone number, IP address, connection speed and, in some cases, information about other devices that are nearby or on their network, so we can do things like help them stream a video from their phone to their TV.

- *Cookie data.* Data from cookies stored on a user's device, including cookie IDs and settings. More information is available at *https://www.facebook.com/policies/cookies/* and *https://help.instagram.com/1896641480634370?ref=ig*.

Advertisers, app developers, and publishers can send us information through Facebook Business Tools they use, including our social plug-ins (such as the Like button), Facebook Login, our APIs and SDKs, or the Facebook pixel. These partners provide information about a person's activities off Facebook—including information about their device, websites they visit, purchases they make, the ads they see, and how they use their services—whether or not they have a Facebook account or are logged into Facebook. For example, a game developer could use our API to tell us what games a person plays, or a business could tell us about a purchase a person made in its store. We also receive information about a person's online and offline actions and purchases from third-party data providers who have the rights to provide us with that person's information.

We use the information we have to deliver our Products, including to personalize features and content (including a person's News Feed, Instagram Feed, Instagram Stories, and ads) and make suggestions for a user (such as groups or events they may be interested in or topics they may want to follow) on and off our Products. To create personalized Products that are unique and relevant to them, we use their connections, preferences, interests, and activities based on the data we collect and learn from them and others (including any data with special protections they choose to provide); how they use and interact with our Products; and the people, places, or things they're connected to and interested in on and off our Products.

For example, if people have shared their device locations with Facebook or checked into a specific restaurant, we can show them ads from an advertiser that wants to promote its services in their area or from the restaurant. We use location-related information—such as a person's current location, where they live, the places they like to go, and the businesses and people they're near—to provide, personalize and improve our Products, including ads, for them and others. Location-related information can be based on things like precise device location (if a user has allowed us to collect it), IP addresses, and information from their and others' use of Facebook Products (such as check-ins or events they attend). We store data until it is no longer necessary to provide our services and Facebook Products, or until a person's account is deleted—whichever comes first. This is a case-by-case determination that depends on things like the nature of the data, why it is collected and processed, and relevant legal or operational retention needs. We provide advertisers with reports about the kinds of people seeing their ads and how their ads are performing, but we don't share information that personally identifies someone (information such as a person's name or e-mail address that by itself can be used to contact them or identifies who they are) unless they give us permission. For example, we provide general demographic and interest information to advertisers (for example, that an ad was seen by a woman between the ages of 25 and 34 who lives in Madrid and likes software engineering) to help them better understand their audience. We also confirm which Facebook ads led people to make a purchase or take an action with an advertiser.

Question 18. There remains concern about timely fixes of security gaps in Facebook. In your written testimony you stated that a feature that allowed user look-up by phone number or e-mail had been abused to scrape profiles and that the feature had recently been shut down. However there are public reports that Facebook was made aware of the vulnerability as early as 2013.

a. Are these reports accurate?

b. If so, why was the feature not fixed earlier?

c. What steps is Facebook taking to ensure that any abuses of privacy are dealt with more expeditiously?

Answer. In April, we found out that a feature that lets users look someone up by their phone number and e-mail may have been misused by browsers looking up people's profiles in large volumes with phone numbers they already had. When we found out about the abuse, we shut this feature down. In the past, we have been aware of scraping as an industry issue, and have dealt with specific bad actors previously.

Question 19. Does Facebook have a specific review protocol for a reported data breach or improper data transfer?

Answer. Yes, Facebook maintains a data incident response plan.

a. If not, why not? Will you be establishing one?

Answer. See response above.

b. If so, what is the protocol? Is there a timeline by which a review should be completed and the vulnerability addressed?

Answer. Facebook monitors its systems for potential breaches of personal data and logs any potential breach in a system that automatically triggers expedited review. Facebook reviews such potential incidents to determine: (i) whether there was in fact an incident, (ii) its root cause, including short-and long-term remediation (if applicable); and (iii) our legal and ethical obligations. Facebook moves quickly to review potential incidents. Because of the fluid nature of an incident, there are no set timelines for completion of reviews and addressing of a discovered vulnerability, but any potential breach is escalated for high priority processing.

c. What are the standards for when and how Facebook will notify users that their information may have been breached or improperly transferred?

Answer. Facebook allows people to view, manage, and remove the apps that they have logged into with Facebook through the App Dashboard. We recently prompted everyone to review their App Dashboard as a part of a Privacy Checkup, and we also provided an educational notice on Facebook to encourage people to review their settings. More information about how users can manage their app settings is available at *https://www.facebook.com/help/218345114850283?helpref=about_content*.

The categories of information that an app can access is clearly disclosed before the user consents to use an app on the Facebook platform. Users can view and edit the categories of information that apps they have used have access to through the App Dashboard.

In addition, Facebook notifies users in accordance with its obligations under applicable law and has also notified people in cases where there was no legal obligation to do so but we nevertheless determined it was the right thing to do under the circumstances.

Question 20. Many of Facebook's vulnerabilities in security or privacy appear to be reported to Facebook and then addressed. Does Facebook have a specific proactive team or protocol for finding security leaks and privacy issues? In short, are there dedicated resources to seek out privacy issues on the platform? If not, why not? If so, when was the proactive approach implemented?

Answer. Protecting a global community of more than 2 billion involves a wide range of teams and functions, and our expectation is that those teams will grow across the board. For example, we have dedicated information security and related engineering teams.

Protecting the security of information on Facebook is at the core of how we operate. Security is built into every Facebook product, and we have dedicated teams focused on each aspect of data security. From encryption protocols for data privacy to machine learning for threat detection, Facebook's network is protected by a combination of advanced automated systems and teams with expertise across a wide range of security fields. Our security protections are regularly evaluated and tested by our own internal security experts and independent third parties. For the past seven years, we have also run an open bug bounty program that encourages researchers from around the world to find and responsibly submit security issues to us so that we can fix them quickly and better protect the people who use our service.

We anticipate continuing to grow these teams by hiring a range of experts, including people with specific types of threat intelligence expertise.

Question 21. How many improper data transfers to third parties have there been?

a. Was Facebook only made aware of the improper data transfers by a third party?

b. Have you ever required an audit to ensure the deletion of improperly transferred data? If so, how many times?

c. Please provide a list of applications that Facebook has previously banned because data was transferred in violation of Facebook's terms.

d. Beyond an audit, what tools is Facebook using to proactively stop improper transfers of data?

e. How are you proactively ensuring that data is not improperly transferred by third parties in the future?

Answer. We launched an initial investigation after the December 11, 2015 publication of an article in *The Guardian* about Cambridge Analytica's potential misuse of Facebook data.

We use a variety of tools to enforce Facebook policies against violating parties, including developers. We review tens of thousands of apps per year and regularly disapprove noncompliant apps as part of our proactive review process. We also use tools like cease and desist letters, account suspensions, letter agreements, and civil

litigation. For example, since 2006, Facebook has sent over 1,150 cease-and-desist letters to over 1,600 targets. In 2017, we took action against about 370,000 apps, ranging from imposing certain restrictions to removal of the app from the platform. Moreover, we have required parties who have procured our data without authorization to delete that data. We have invested significant resources in these efforts. Facebook is presently investigating apps that had access to large amounts of information before we changed our platform policies in 2014 to significantly reduce the data apps could access. To date around 200 apps (from a handful of developers: Kogan, AIQ, Cube You, the Cambridge Psychometrics Center, myPersonality, and AIQ) have been suspended—pending a thorough investigation into whether they did in fact misuse any data.

Question 22. In page 3 of your written testimony you state that "strict requirements" are going to be put on developers. What are those strict requirements?

Answer. Recently, we announced a number of additional steps we're taking to address concerns raised by Kogan's app.

- *Review our platform.* We are investigating all apps that had access to large amounts of data before the platform changes we announced in 2014, and we will audit any app where we identify suspicious activity. If we identify misuses of data, we'll take immediate action, including banning the app from our platform and pursuing legal action if appropriate.
- *Tell people about data misuse.* We will tell people about apps that have misused their data.
- *Turn off access for unused apps.* If someone has not used an app within the last three months, we will turn off the app's access to their data.
- *Restrict Facebook Login data.* We are changing Login, so that the only data that an app can request without app review will include name, profile photo, and e-mail address. Requesting any other data will require approval from Facebook. We will also no longer allow apps to ask for access to information like religious or political views, relationship status and details, custom friends lists, education and work history, fitness activity, book reading and music listening activity, news reading, video watch activity, and games activity. We will encourage people to manage the apps they use. We already show people what apps their accounts are connected to and allow them to control what data they've permitted those apps to use. But we're making it easier for people to see what apps they use and the information they have shared with those apps.
- *Reward people who find vulnerabilities.* We launched the Data Abuse Bounty program so that people can report to us any misuses of data by app developers.
- *Update our policies.* We have updated our terms and Data Policy to explain in more detail how we use data and how data is shared with app developers.

Question 23. Please list all the companies or persons to whom Aleksandr Kogan sold Facebook data.

Answer. Kogan represented that, in addition to providing data to his Prosociality and Well-Being Laboratory at the University of Cambridge for the purposes of research, GSR provided some Facebook data to SCL Elections Ltd., Eunoia Technologies, and the Toronto Laboratory for Social Neuroscience at the University of Toronto. However, the only party Kogan has claimed paid GSR was SCL. Our investigation is ongoing.

Question 24. Please provide a detailed account of why Facebook did not detect that Mr. Kogan's user agreement included an agreement for resale, in violation of Facebook's polices?

Answer. Facebook has developed an automated system for checking that all apps had terms of service and data policies. In performing such checks, however, Facebook does not examine the content of the developers' terms and policies because app developers act as independent third parties with regard to the data they obtain; they determine the purposes for which, and the manner in which, that data is processed. Our understanding is that this is consistent with the practices of other major online and mobile platforms, which generally enable developers on their platforms to provide access to the developers' terms and policies in their app stores, but do not proactively review the substance of those policies.

Although developers act as independent third parties with regard to the data users share with them, all apps on the Facebook Platform must comply with our user data policies, Community Standards, Platform Policies, and Ad Guidelines. Our Platform policy also contains a number of enforcement provisions which apply after an app has been reviewed and approved. Facebook has several teams dedicated to detecting, escalating, investigating, and combating violations of its policies, includ-

ing schemes to improperly access, collect, or exploit user data. The Developer Operations Policy Enforcement team looks for policy violations and either brings developers into compliance or removes them from the platform, and the Developer Operations Review team conducts an upfront review of apps to confirm proper use of advanced permissions.

Question 25. What information exactly was received by Aleksandr Kogan? Private messages? Friends of friends' info?

Answer. Approximately 300,000 Facebook users worldwide installed Kogan's app. For the majority of these users, the app requested consent to access the following data fields associated with the user and with the friends of the user: Public profile data, including name and gender; Birthdate; "Current city" in the "About" section of the user's profile, if provided; and Facebook Pages liked.

For a small subset of users, it appears that the app also requested consent to access users' Facebook messages (fewer than 1,500 individuals, based on current information) and to posts that appeared in the user's News Feed or Timeline (approximately 100 individuals, based on current information)—but only for users who installed the app. For a small subset of users (fewer than 1,500 individuals, based on current information), it appears that the app also requested consent to access the hometowns that the users' friends had specified in the "About" section of their profiles. And for a handful of people (fewer than 10) who appear to be associated with Kogan/GSR, the app requested consent to e-mail address and photos.

Question 26. Does Facebook have any evidence or reason to believe Cambridge Analytica, GSR, or Kogan, retained Facebook data after they certified they had deleted it?

Answer. In March 2018, we learned from news reports that contrary to the certifications given, not all of the Kogan data may have been deleted by Cambridge Analytica. We have no direct evidence of this and no way to confirm this directly without accessing Cambridge Analytica's systems and conducting a forensic audit. We have held off on audits of Cambridge Analytica and other parties that are being investigated by the UK Information Commissioner's Office at its request. Our investigation is ongoing.

Question 27. Are you currently engaged in any industry-wide conversations about setting best practices for disclosures of data collection and use, privacy policy settings, and/or proactively discovering privacy lapses? If not, why not? If so, will a public report be generated? If so, when?

Answer. We regularly consult with a range of experts in our effort to deliver and improve the strong privacy protections that people who use Facebook expect. This includes regular consultation with privacy experts, academics, other companies, and industry groups. While we recognize that there is no one-size-fits-all approach to strong privacy protections, we believe that these ongoing discussions better enable us to design our services in a way that responds to the feedback we're receiving, as well as new research and best practices around privacy.

Question 28. Please provide a detailed breakdown of the principles that will guide the development of artificial intelligence (AI) practices, the details about what those practices are, and how they'll help users.

Answer. We are focused on both the technical and the ethical aspects of artificial intelligence. We believe these should go hand-in-hand together in order to fulfill our commitment to being fair, transparent, and accountable in our development and use of AI. Facebook has AI teams working on developing the philosophical, as well as technical, foundations for this work. Facebook is also one of the co-founders and members of the Partnership on AI (PAI), a collaborative and multi-stakeholder organization established to study and formulate best practices on AI technologies, to advance the public's understanding of AI, and to serve as an open platform for discussion and engagement about AI and its influences on people and society. The thematic pillars that structure the work we're doing in the scope of the PAI—safety, fairness, transparenc,y and accountability—are the principles that we believe industry should follow and promote when building and deploying AI systems. The PAI's Fair, Transparent and Accountable AI Working Group is also working alongside industry, academia and civil society to develop best practices around the development and fielding of fair, explainable, and accountable AI systems.

a. Many are skeptical AI will be a cure-all for content issues. Facebook has also announced it will hire more content reviewers. Does Facebook have any other plans to deal with content review?

Answer. We believe that over the long term, building AI tools is the scalable way to identify and root out most of this harmful content. We're investing a lot in building those tools. And we already use artificial intelligence to help us identify threats of real world harm from terrorists and others. For example, the use of AI and other

automation to stop the spread of terrorist content is showing promise. Today, 99 percent of the ISIS and Al Qaeda related terror content we remove from Facebook is content we detect before anyone in our community has flagged it to us, and in some cases, before it goes live on the site. We do this primarily through the use of automated systems like photo and video matching and text-based machine learning. We also use AI to help find child exploitation images, hate speech, discriminatory ads, and other prohibited content. Moreover, in the last year, we have basically doubled the number of people doing security and content review. We will have more than 20,000 people working on security and content review by the end of this year.

b. You have offered a "bounty" for information about improperly transferred user data. Are you concerned this bounty program may promote the hacking of third-party app developers? Could offering small bounties for finding hate speech, terrorism, etc. encourage more user reporting on the platform?

Answer. The Data Abuse Bounty Program is carefully designed to help us lawfully obtain data necessary to review apps that are operating from malicious intent of their developers. The program does not reward reports that were a direct or indirect result of hacking of third-party app developers. We made this explicitly clear in the terms of the program. Following an investigation, we will reward a submission only if the report is genuine, based on direct and personal knowledge, and the information was obtained lawfully. To prevent abuse, we require the submission to be submitted in narrative form without any data appended. We will request data only if we need it and we are absolutely confident that the reporter obtained it and can share it lawfully.

The Data Abuse Bounty will reward people with first-hand knowledge and proof of cases where a Facebook platform app collects and transfers people's data to another party to be sold, stolen or used for scams or political influence. We'll review all legitimate reports and respond as quickly as possible when we identify a credible threat to people's information. If we confirm data abuse, we will shut down the offending app and, if necessary, take legal action against the company selling or buying the data. We'll pay a bounty to the person who reported the issue, or allow them to donate their bounty to a charity, and we'll also alert those we believe to be affected. We also encourage our users to report to us content that they find concerning or that results in a bad experience, as well as other content that may violate our policies. We review these reports and take action on abuse, like removing content and disabling accounts.

Question 29. Do you have a specific office that can respond to users' complaints and questions regarding privacy? If so, how is this office advertised? Could it be made more accessible to the public and or better equipped? If you have no such office, why not?

Answer. Yes. In addition to the range of online educational resources that we provide through our website and mobile apps, we have staff responsible for responding to questions from people about privacy. We distribute the contact information for this team in a number of ways, including in the section of our Data Policy that begins with the heading, "How to contact Facebook with questions."

Question 30. What assistance do Facebook employees embedded with advertising and political clients provide?

Answer. Facebook representatives advise political advertisers on Facebook, as they would with other, non-political managed accounts. During the 2016 election cycle, for example, Facebook provided technical support and best practices guidance on optimizing their use of Facebook.

a. Is there any way these embedded persons could bypass a security or privacy feature?

b. Has Facebook investigated whether any Facebook personnel assisting the Obama campaign violated any Facebook policies?

c. What protocols are in place to make sure these embedded persons cannot take any steps to bypass privacy or security controls on Facebook?

Answer. Both the Obama and Romney campaigns had access to the same tools, and no campaign received any special treatment from Facebook. We continuously work to ensure that we comply with all applicable laws and policies.

Question 31. You have received numerous questions about removing conservative content from Facebook. You have answered that these were enforcement errors.

a. Have you undertaken any study to determine whether any specific forms of content have been more or less likely to be removed? If not, why not? If so, what are the results? Have you found that conservative content is more likely to be removed?

b. What is the source of the enforcement errors? Are these individual people, AI algorithms, or something else?

c. How are you addressing the source of any errors? E.g., training for individuals, changes to the AI algorithm?

d. How do you notify persons whose content has been deleted of the deletion and the reasons for it?

e. Do you disconnect friends with deleted content?

f. Do you prevent information from reaching the feed of followers of persons who have previously had content deleted?

g. How quickly are complaints about improper censoring addressed?

h. How quickly are complaints about threats addressed?

Answer. Suppressing political content or preventing people from seeing what matters most to them is directly contrary to Facebook's mission and our business objectives.

We have engaged an outside advisor, former Senator Jon Kyl, to advise the company on potential bias against conservative voices. We believe this external feedback will help us improve over time and ensure we can most effectively serve our diverse community.

We recently published a detailed set of Community Standards—which reflect our internal reviewer guidelines—to help people understand where we draw the line on complex and nuanced issues. Publishing these details will also make it easier for everyone to give us feedback so that we can improve the guidelines—and the decisions we make—over time. Our Community Standards, which are designed to encourage expression and create a safe environment on Facebook, outline what is and isn't allowed on the platform.

When someone violates our Community Standards, we send them a notification. We are also introducing the right to appeal our decisions on individual posts so people can ask for a second opinion when they think we've made a mistake.

Question 32. How do you as a company deal with a person whose content was wrongly deleted? Do you simply restore the content? Do you offer an apology? Do you make any form of recompense, or otherwise make clear to the user their speech is welcome on the platform?

Answer. We recognize that our policies are only as good as the strength and accuracy of our enforcement—and our enforcement is not perfect. We make mistakes because our processes involve people, and people are not infallible. We are always working to improve.

When we're made aware of incorrect content removals, we review them with team members so as to prevent similar mistakes in the future. On April 24, 2018, we announced the launch of appeals for content that was removed for hate speech. We recognize that we make enforcement errors on both sides of the equation—what to allow, and what to remove—and that our mistakes cause a great deal of concern for people, which is why we need to allow the option to request review of the decision and provide additional context that will help our team see the fuller picture as they review the post again. This type of feedback will allow us to continue improving our systems and processes so we can prevent similar mistakes in the future.

We also audit the accuracy of reviewer decisions on an ongoing basis to coach them and follow up on improving where errors are being made.

We hope that our recent decision to publicize our detailed Community Standards, reflecting our internal reviewer guidelines, and the introduction of appeals will aid in this process. By providing more clarity on what is and isn't allowed on Facebook, we hope that people will better understand how our policies apply to them. For some violation types, where people believe we have made a mistake, they can request review of our decisions, and we are working to extend this process further by supporting more violation types.

Question 33. During the hearing, you testified that Facebook will soon, or does, employ 20,000 personnel to work exclusively on content moderation.

a. How many personnel currently work on content moderation? How many new personnel must you hire to reach 20,000?

b. Will all new personnel be directly employed by Facebook?

i. If the answer to question b is no, what percentage of new personnel will be employed directly by Facebook?

ii.What percentage will be employed by a third party?

c. For all new personnel, whether employed directly by Facebook or by a third party, how many will be American citizens?

i. How many new personnel will be foreign nationals?

ii. For all new personnel who are foreign nationals, what worker visa programs—including but not limited to the H–1B and TN visa programs—will Facebook or a third party use? Please provide a list of every specific worker visa program Facebook or a third party intends to use for employment purposes.

iii. What steps will Facebook take to ensure that both the spirt and the letter of the law governing any worker visa program is complied with, both by Facebook itself and any third party?

iv. What additional measures will Facebook or any contracted third party take to ensure that American workers are not displaced by foreign workers?

v. What additional measures will Facebook or any contracted third party take to ensure that foreign workers are not paid a lower wage than their American counterparts?

vi. Will you commit that no American workers will lose their job as a result of Facebook or a contracted third party employing a foreign worker?

Answer. Today, we have about 15,000 people working on security and content review across the company.

Of that 15,000, more than 7,500 people review content around the world.

- Our content review team is global and reviews reports in over 50 languages.
- Reports are reviewed 24 hours a day, 7 days a week and the vast majority of reports are reviewed within 24 hours.
- Our goal is always to have the right number of skilled people with the right language capabilities to ensure incoming reports are reviewed quickly and efficiently.
- We hire people with native language and other specialist skills according to the needs we see from incoming reports.
- The team also includes specialists in areas like child safety, hate speech and counter-terrorism, software engineers to develop review systems, quality control managers, policy specialists, legal specialists, and general reviewers.

To provide 24/7 coverage across dozens of languages and time zones and ensure that Facebook is a place where both expression and personal safety are protected and respected, our content review team includes a combination of employees, contractors, and vendor partners based in locations around the world.

Facebook endeavors to comply with all applicable immigration laws in the United States and the other countries where we operate.

Question 34. What regulations would Facebook support?

Answer. Facebook is generally not opposed to regulation but wants to ensure it is the right regulation. The issues facing the industry are complex, multi-faceted, and affect an important part of peoples' lives. As such, Facebook is absolutely committed to working with regulators, like Congress, to craft the right regulations. Facebook would be happy to review any proposed legislation and provide comments.

RESPONSE TO WRITTEN QUESTIONS SUBMITTED BY HON. ORRIN HATCH TO MARK ZUCKERBERG

Question 1. I understand that until just recently, Facebook split its privacy policy across 20 or more separate webpages, making it virtually impossible for a typical user to understand what information he or she was agreeing to allow Facebook to share. Why did you have in place such a convoluted privacy policy? Why not make the policy as clear, easy to understand, and accessible as possible?

Answer. We've heard loud and clear that it's important to make privacy information and controls easy for people to find and use. We've made recent improvements to our privacy settings to centralize people's choices, and are providing access to people's key privacy choices through an updated Privacy Shortcuts feature.

With regard to our Data Policy specifically, it has been available in a single webpage for many years. We recently updated our Data Policy in response to feedback that, among other things, we should provide more detailed explanations and improve the design of the policy. Like its predecessor, this policy is framed around short, easy-to-understand topics and questions, like "What kinds of information do we collect" and "How can I manage or delete information about me."

In designing both our newly updated Data Policy and its predecessor, as well as our Privacy Basics educational center, we were mindful of guidance from the FTC and many other experts that recommend so-called "layered" privacy policies, which

make it easy to find topics and high-level information but enable people to access more detailed information if they wish to do so.

Question 2. I've been a bit perplexed by the way Facebook has come in for such criticism when so many other online platforms use a similar business model. I don't necessarily want to name names here, but Facebook is far from the only website that makes money by offering advertisers the ability to target ads to specific user groups. How does your business model differ from, say, Google's, or from other social media sites?

Answer. Like many other free online services, we sell advertising space to third parties. Doing so enables us to offer our services to consumers for free. This is part of our mission to give people the power to build community and bring the world closer together.

Question 3. Is Facebook unique in the way it collects user information and offers targeted advertising? How do your data practices differ from those of other websites?

Answer. No. Countless online and offline companies sell and display advertising to support the costs of their services, and most engage in a variety of practices (targeting, contextual placement, list management) to deliver the most relevant and cost-effective advertising to people and businesses. Ad-based business models have long been a common way to enable companies to offer free services, even before the advent of the Internet when media like radio, television, and newspapers were ad-supported. Online advertising is particularly important for smaller and more niche publishers, as well as services—like Facebook—whose mission is to provide access to everyone, regardless of their location or ability to pay for services.

While we provide similar services to other websites—and to the third-party providers of online advertising services on which many websites rely—we are unique in the level of control we offer over how we use information to deliver ads. For example, we launched an About Facebook Ads page (*www.facebook.com/ads/about*) that explains how we use information to deliver Facebook ads. Every ad on Facebook comes with a "Why am I seeing this?" tool that lets people learn why they are seeing that particular ad, and to control whether they would like to see similar ads in the future. And we have built a comprehensive Ad Preferences tool, which enables people to see interests that we use to decide what ads to show people, and the list of advertisers that are showing people ads on Facebook because of past interactions with the advertiser.

Although these features exceed the transparency and control offered by many other companies, we've heard that we need to continue to invest in improvements in this area. That's why, among other things, we've announced plans to build Clear History, a new feature that will enable users to see the websites and apps that send us information when they use them, delete this information from their accounts, and turn off our ability to store it associated with their accounts going forward.

Question 4. Does Facebook *ever* share user data with advertisers? If so, in what circumstances does Facebook share such data? Do advertisers ever learn the names of, or identifying information about, the individuals who receive their advertisements?

Answer. We provide advertisers with reports about the kinds of people seeing their ads and how their ads are performing, but we don't share information that personally identifies people (information such as name or that by itself can be used to contact or identifies a person) unless we have permission from people. For example, we provide statistical demographic information to advertisers (for example, that an ad was seen by 2,436 women between the ages of 25 and 34 in Maryland) to help them better understand their audience. We also confirm which Facebook ads led people to make purchases or take an action with an advertiser.

Question 5. How would limiting Facebook's ability to offer targeted advertising change your business model? How would it impact the services you offer to customers?

Answer. To build a secure product with extensive infrastructure that connects people across continents and culture, we need to make sure everyone can afford it. To do this, we sell advertising, and we could not offer our service for free without selling advertising. Advertising lets us keep Facebook free, which ensures it remains affordable for everyone.

Separately, our core service involves personalizing all content, features, and recommendations that people see on Facebook services. No two people have the same experience on Facebook or Instagram, and they come to our services because they expect everything they see to be relevant to them. If we were not able to personalize or select ads or other content based on relevance, this would fundamentally change the service we offer on Facebook—and it would no longer be Facebook.

Question 6. In your written testimony, you discuss new efforts to verify advertisers who want to run political or issue ads on Facebook. It strikes me that this effort should apply to more than just political ads. For example, shouldn't you also put in place checks for advertisers that use your platform to illegally peddle prescription drugs? Which advertisers will need to be verified under your new policies? And how can we be sure that Facebook won't use these new policies to engage in viewpoint discrimination?

Answer. Last October, we announced that we would require advertisers running electoral ads to verify their identities and locations. We also announced that we would require these ads to use a "paid for by" label and that we would include them in a searchable archive. In April, we announced that we would extend these transparency measures to "issue ads"—ads about national policy issues. We have worked with third parties like the Comparative Agendas Project to define an initial set of issues, and we will refine that list over time.

RESPONSE TO WRITTEN QUESTIONS SUBMITTED BY HON. DIANNE FEINSTEIN TO MARK ZUCKERBERG

Scraping of Public Profiles

Question 1. Nearly 2.2 billion people who use Facebook[1] have likely had their public profiles scraped by malicious actors, including by use of a search feature that allowed people to use telephone numbers and e-mail addresses to obtain user information and through the company's account recovery feature.

a. Why didn't Facebook take any action when it learned in 2013[2] that malicious actors could use its features to obtain personal information from users' profile pages?

b. Facebook has now disabled the search feature, but are there plans to replace it? If so, what has Facebook done to ensure that personal information cannot be obtained using this new search feature?

c. What changes is Facebook making to the account recovery feature to reduce the risk that personal information will be accessible to malicious actors?

d. What steps is Facebook taking to protect its 2.2 billion users whose information may have been scraped by malicious actors?

e. What information is being provided to users?

Answer. In April, we found out that a feature that lets users look someone up by their phone number and e-mail may have been misused by browsers looking up people's profiles in large volumes with phone numbers they already had. When we found out about the abuse, we shut this feature down. In the past, we have been aware of scraping as an industry issue, and have dealt with specific bad actors previously.

Third Parties

Question 2. In 2014, Facebook updated its policies to reduce third party applications' access to user data. Facebook is now investigating applications that, as you described had access to "a large amount of information," before this change.

a. How is Facebook defining "a large amount of information?"

Answer. Our investigation is ongoing and as part of it we are taking a close look at applications that had access to friends data under Graph API v.1.0 before we made technical changes to our platform to change this access.

b. How is Facebook determining what applications to include in this investigation?

Answer. We are in the process of investigating every app that had access to a large amount of information before we changed our Platform in 2014. The investigation process is in full swing, and it has two phases. First, we are undertaking a comprehensive review to identify every app that had access to this amount of Facebook data and to focus on apps that present reason for deeper investigation. And second, where we have concerns, we will conduct interviews, make requests for information (RFI)—which ask a series of detailed questions about the app and the data it has access to—and perform audits using expert firms that may include on-site inspections. We have large teams of internal and external experts working hard to investigate these apps as quickly as possible. To date thousands of apps have been inves-

---

[1] Throughout these Questions, references to Facebook refer to Facebook as well as all other Facebook-owned platforms, products, applications, and subsidiaries. For example, this includes Instagram and WhatsApp.

[2] *See, e.g.*, Matt Burgess, "Facebook fixed a massive data scraping issue it said wasn't a problem," Wired UK (Apr. 5, 2018).

tigated and around 200 apps have been suspended—pending a thorough investigation into whether they did in fact misuse any data. Where we find evidence that these or other apps did misuse data, we will ban them and let people know.

These apps relate to a handful of developers: Kogan, AIQ, Cube You, the Cambridge Psychometrics Center, and myPersonality, with many of the suspended apps being affiliated with the same entity. Many of these suspensions include apps that appear to be "test" apps that were never released to the public, and therefore would not have acquired significant user data, although our investigation into these apps is ongoing.

Additionally, we have suspended an additional 14 apps, which were installed by around one thousand people. They were all created after 2014, after we made changes to more tightly restrict our platform APIs to prevent abuse. However, these apps appear to be linked to AIQ, which was affiliated with Cambridge Analytica. So we have suspended them while we investigate further. Any app that refuses to take part in or fails our audit will be banned.

c. When do you estimate this investigation will be complete?

Answer. It's going to take many months to do this full process.

d. Will Facebook make public the results of this investigation? If not, why not and will you notify Congress and provide the results when you are done?

Answer. Where we find evidence that these or other apps did misuse data, we will ban them from the platform and tell people who used or may have had data shared with the app.

e. How will Facebook notify people whose data was improperly used?

Answer. See Response to Question (d).

f. What is Facebook doing to monitor and investigate whether developers or others are taking and selling personal information?

Answer. In general, on an ongoing basis, we proactively review all apps seeking access to more than basic information (and have rejected more than half of apps seeking such extended permissions). We also do a variety of manual and automated checks to ensure compliance with our policies and a positive experience for people. These include steps such as random checks of existing apps along with the regular and proactive monitoring of apps. We also respond to external or internal reports and investigate for potential app violations. When we find evidence of or receive allegations of violations, we investigate and, where appropriate, employ a number of measures, including restricting applications from our platform, preventing developers from building on our platform in the future, and taking legal action where appropriate.

Question 3. Individuals who use Facebook assume a certain level of privacy. There may be an understanding that if something posted is "public" that it's available broadly. However, the amount of data and personal information available through your platforms is enormous.

a. What data about individuals, if any, does Facebook make available to businesses?

Answer. Facebook does not sell people's information to anyone, and we never will. We also impose strict restrictions on how our partners can use and disclose the data we provide.

Our Data Policy makes clear the circumstances in which we work with third parties who help us provide and improve our Products or who use Facebook Business Tools to grow their businesses, which makes it possible to operate our companies and provide free services to people around the world.

When people choose to use third-party apps, websites, or other services that use, or are integrated with, our Products, they can receive information about what users post or share. For example, when users play a game with their Facebook friends or use a Facebook Comment or Share button on a website, the game developer or website can receive information about the users' activities in the game or receive a comment or link that users share from the website on Facebook. Also, when users download or use such third-party services, they can access users' public profile on Facebook, and any information that users share with them. Apps and websites that people use may receive their list of Facebook friends if they choose to share it with them. But apps and websites that people use will not be able to receive any other information about their Facebook friends from users, or information about any of the users' Instagram followers (although friends and followers may, of course, choose to share this information themselves). Information collected by these third-party services is subject to their own terms and policies.

Devices and operating systems providing native versions of Facebook and Instagram (*i.e.,* where we have not developed our own first-party apps) will have access to all information people choose to share with them, including information

that friends share with users, so they can provide our core functionality to our users.

b. Can businesses access users' e-mails, direct messages, buying history, or credit card information?

Answer. See Response to Question 3, part a.

c. Your privacy policies indicate Facebook collects the content of messages through your direct messenger applications and through private group postings. How is that information used? Is it shared with anyone?

Answer. We use the information we collect for purposes specified in our Data Policy. These purposes include:

- Providing, personalizing and improving our products;
- Providing measurement, analytics and other business services;
- Promoting safety, integrity and security;
- Communicating with our community;
- Conducting research and innovating for social good.

d. Does Facebook have the capacity to monitor how researchers or businesses use data they get from Facebook?

Answer. We have a variety of controls in place to help ensure researchers and businesses comply with our policies.

e. What does Facebook do, if anything, to ensure researchers and others comply with its use agreements?

Answer. If we discover a researcher or business has misused people's information, we take appropriate action to address the issue. Such action may include suspending the business from Facebook or even banning it altogether.

f. What limitations has Facebook placed on the personal information that application developers can request from Facebook users? How is this enforced?

Answer. In April 2014, we announced that we would more tightly restrict our platform APIs to prevent abuse. At that time we made clear that existing apps would have a year to transition—at which point they would be forced (1) to migrate to the more restricted API and (2) be subject to Facebook's new review and approval protocols. A small number of developers asked for and were granted short-term extensions beyond the one-year transition period, the longest of which lasted several months. These extensions ended several years ago. A transition period of this kind is standard when platforms implement significant changes to their technology base and was necessary here to avoid disrupting the experience of millions of people. New apps that launched after April 30, 2014 were required to use our more restrictive platform APIs.

We are further restricting the data that an app can access without review to a person's name, profile photo, and e-mail address. We review to ensure that the requested permissions clearly improve the user experience and that the data obtained is tied to an experience within the app. We conduct a variety of manual and automated checks of applications on the platform for Policy compliance, as well as random sampling. When we find evidence of or receive allegations of violations, we investigate and, where appropriate, employ a number of measures, including restricting applications from our platform, preventing developers from building on our platform in the future, and taking legal action where appropriate.

g. What limits has Facebook placed on how personal information can be used by third parties? Has Facebook prohibited uses beyond what is necessary to run third party applications?

Answer. Developers can access Account Information in accordance with their privacy policies and other Facebook policies. All other data may not be transferred outside the Facebook app, except to service providers, who need that information to provide services to the Facebook app. With the exception of Account Information, developers may only maintain user data obtained from Facebook for as long as necessary for their business purpose. Developers may not use data obtained from Facebook to make decisions about eligibility, including whether to approve or reject an application or how much interest to charge on a loan. Developers must protect the information they receive from Facebook against unauthorized access, use, or disclosure. For example, developers may not use data obtained from Facebook to provide tools that are used for surveillance.

Cambridge Analytica

Question 4. Facebook learned in 2015 that Cambridge Analytica had obtained Facebook user information without notice or consent.

a. Why didn't Facebook notify users of this breach in 2015?

b. What is Facebook's current policy for notifying users of privacy breaches?

c. Why didn't Facebook suspend or ban Cambridge Analytica from its platforms until 2018?

d. Why didn't Facebook audit Cambridge Analytica?

e. What led Facebook to consider the matter "closed" without taking any of these steps?

f. Have there been any reforms to Facebook's internal investigative policies based on this experience? (If so, please describe these changes.)

g. Why didn't Facebook notify the Federal Trade Commission of this incident before press stories broke in March 2018?

h. What will Facebook do to protect the 87 million people whose personal information remains in the hands of third parties? [3]

Answer. When Facebook learned in December 2015 of allegations that Kogan may have violated Facebook's policies, we took immediate action. Facebook immediately banned Kogan's app from our developer platform and retained an outside firm to investigate what happened and what further action we should take to enforce our Platform Policies and protect people. This culminated in certifications from Kogan, and from Cambridge Analytica and others whom he certified he had shared some data with, certifying that they had deleted all data and any derivatives of the data. Because Kogan's app could no longer obtain access to most user data (or any friends data) in December 2015 due to changes in Facebook's platform, the most responsible step to protect users at the time was to work with Kogan, Cambridge Analytica, and others to obtain deletion of the data.

Although our developer terms gave us the ability to audit Kogan's app, we did not have an agreement in place that would have allowed us to audit third parties that he may have shared data with. For this reason, we chose to require him to obtain certifications of deletion from each of these parties, leveraging our rights as to Kogan, who was the developer of the app.

In March 2018, Facebook received information from the media that possible questions existed around the validity of deletion certifications that Facebook received. In response, Facebook immediately banned Cambridge Analytica and other potentially related parties from distributing advertising on Facebook or from using other aspects of our service. At that time, we requested an on-site audit of Cambridge Analytica, which it agreed to. The forensic auditor's work is currently on hold at the request of U.K. regulatory authorities, who themselves are investigating Cambridge Analytica, which is located in the U.K., and we are actively cooperating with the U.K. authorities to progress this analysis.

It is important to clarify that Kogan's improper disclosure of Facebook data that users shared with him does not involve a data breach on Facebook's platform. There was no unauthorized access to Facebook data by Kogan, and instead, his app could only access Facebook data that users specifically consented to share with him. Even though Kogan's improper disclosure of data was not a breach of our systems, these actions violate our Platform policy—and we took extensive measures to try to mitigate any potential misuse of that data by downstream parties by pushing aggressively for deletion. And we are implementing an approach that goes beyond legal requirements and informs people any time we learn than an app developer shared data with a third-party in violation of our policies. This is consistent with the responsibility we believe we have with our users, even if the law does not require this.

Question 5. Cambridge Analytica whistleblower Christopher Wylie told the U.K.'s House of Commons that senior employees at another data analytics firm were also working on the Facebook data obtained through Aleksandr Kogan's application.

a. Did anyone besides Prof. Kogan and Cambridge Analytica have access to the data obtained by Prof. Kogan?

b. Does any company have that data today?

c. What steps are you taking to find out who had access to the data and how it was used?

d. Is this data still being used? How can its ongoing use be prevented?

Answer. On December 11, 2015, The Guardian published an article reporting that Kogan and his company, GSR, may have passed information the app had obtained

[3] *See, e.g.,* Matthew Rosenberg *et al.,* "How Trump Consultants Exploited the Facebook Data of Millions," *N.Y. Times* (Mar. 17, 2018) (the *New York Times* viewed raw data from the profiles Cambridge Analytica obtained; copies of the data remain on Cambridge Analytica servers); Channel 4, "Revealed: Cambridge Analytica data on thousands of Facebook users still not deleted," (Mar. 28, 2018) (Channel 4 News saw data on thousands of people in Colorado).

from Facebook users to SCL Elections Ltd. (SCL)/Cambridge Analytica. If this occurred, Kogan and his company violated Facebook's Platform Policies, which explicitly prohibited selling user data accessed from Facebook and from sharing any user data accessed from Facebook with any ad network, data broker or other advertising or monetization related service.

For this reason, Facebook immediately banned the app from our platform and investigated what happened and what further action we should take to enforce our Platform Policies. Facebook also contacted Kogan/GSR and demanded that they explain what data they collected, how they used it, and to whom they disclosed it. Facebook further insisted that Kogan and GSR, as well as other persons or entities to whom they had disclosed any such data, account for and irretrievably delete all such data and information.

Facebook also contacted Cambridge Analytica to investigate the allegations reflected in the reporting. On January 18, 2016, Cambridge Analytica provided written confirmation to Facebook that it had deleted the data received from Kogan and that its server did not have any backups of that data. On June 11, 2016, Kogan executed and provided to Facebook signed certifications of deletion on behalf of himself and GSR. The certifications also purported to identify all of the individuals and entities that had received data from GSR (in addition to Kogan and his lab), listing the following: SCL, Eunoia Technologies (a company founded by Christopher Wylie), and a researcher at the Toronto Laboratory for Social Neuroscience at the University of Toronto. On July 7, 2016, a representative of the University of Toronto certified that it deleted any user data or user-derived data. On August 16, 2016, Eunoia (executed by Eunoia Founder Christopher Wylie) certified that it deleted any user and user-derived data. On September 6, 2016, counsel for SCL informed counsel for Facebook that SCL had permanently deleted all Facebook data and derivative data received from GSR and that this data had not been transferred or sold to any other entity. On April 3, 2017, Alexander Nix, on behalf of SCL, certified to Facebook, that it deleted the information that it received from GSR or Kogan.

Because all of these concerns relate to activity that took place off of Facebook and its systems, we have no way to confirm whether Cambridge Analytica may have Facebook data without conducting a forensic audit of its systems. Cambridge Analytica has agreed to submit to a forensic audit, but we have not commenced that yet due to a request from the UK Information Commissioner's Office, which is simultaneously investigating Cambridge Analytica (which is based in the UK). And even with an audit, it may not be possible to determine conclusively what data was shared with Cambridge Analytica or whether it retained data after the date it certified that data had been deleted.

The existing evidence that we are able to access supports the conclusion that Kogan only provided SCL with data on Facebook users from the United States. While the accounts of Kogan and SCL conflict in some minor respects not relevant to this question, both have consistently maintained that Kogan never provided SCL with any data for Facebook users outside the United States. These consistent statements are supported by a publicly released contract between Kogan's company and SCL.

Question 6. Cambridge Analytica's managing director was recorded explaining that the company pushes propaganda "into the bloodstream of the internet, and then watch[es] it grow, give[s] it a little push every now and again . . . like a remote control."[4]

a. Has Facebook investigated what material Cambridge Analytica put on Facebook's platforms, how the material spread, and how Cambridge Analytica targeted people?

b. If yes, please provide your findings to the Committee.

c. If not, will Facebook conduct this investigation or allow researchers to do this, and to provide the findings to the Committee?

Answer. Our investigation of Cambridge Analytica's advertising activities is ongoing, and we have banned Cambridge Analytica from purchasing ads on our platform. Cambridge Analytica generally utilized custom audiences, some of which were created from contact lists and other identifiers that it generated and uploaded to our system to identify the people it wanted to deliver ads to on Facebook, and in some instances, refined those audiences with additional targeting attributes.

Question 7. Cambridge Analytica and the Kremlin-backed Internet Research Agency both improperly targeted Facebook users to influence the 2016 election.

---

[4] Sonam Sheth, "Cambridge Analytica began testing out pro-Trump slogans the same year Russia launched its influence operation targeting the 2016 election," Business Insider (Mar. 20, 2018).

a. Has Facebook compared Cambridge Analytica's targeting of Facebook users in the United States during the 2016 presidential election cycle to targeting by the Internet Research Agency?

b. If yes, please describe how Cambridge Analytica's targeting was both similar to and different from the Internet Research Agency's targeting.

c. If not, will Facebook do this, and provide its findings to the Committee?

Answer. The targeting for the IRA ads that we have identified and provided to the Senate Committee on the Judiciary and the Senate Select Committee on Intelligence was relatively rudimentary, targeting very broad locations and interests, and for example, only used custom audiences in a very small percentage of its overall targeting and did not use Contact List Custom Audiences. In addition, all of the custom audiences used by the IRA were created based on user engagement with certain IRA pages. By contrast, Cambridge Analytica used hundreds of Contact List Custom Audiences during the 2016 election cycle created from contact lists that Cambridge Analytica uploaded to our system, and Cambridge Analytica used those and other custom audiences in the majority of its ads targeting in combination with demographic targeting tools.

Foreign Actors

Question 8. A new study found that more than half of the sponsors of Facebook ads that featured divisive political messages during the 2016 election were from "suspicious" groups, and that one in six suspicious advertisers was linked to the Internet Research Agency.[5]

a. Will you work with these researchers to determine whether any of the "suspicious groups" they identified, other than those associated with the Internet Research Agency, are also linked to Russia or other foreign government actors?

b. If so, please also provide the findings to this Committee.

c. If not, will you perform your own analysis of who bought divisive issue ads leading up to the 2016 election, including how many were attributable to the Internet Research Agency or other Russian-backed accounts, and provide your findings to the Committee?

Answer. Facebook has conducted a broad search for evidence that Russian actors, not limited to the IRA or any other specific entity or organization, attempted to interfere in the 2016 election by using Facebook's advertising tools. We found coordinated activity that we now attribute to the IRA, despite efforts by these accounts to mask the provenance of their activity. We have used the best tools and analytical techniques that are available to us to identify the full extent of this malicious activity, and we continue to monitor our platform for abuse and to share and receive information from others in our industry about these threats.

We will continue to work with the government, and across the tech industry and civil society, to address this important national security matter so that we can do our part to prevent similar abuse from happening again. That's why we have provided all of the ads and associated information to the committees with longstanding, bipartisan investigations into Russian interference, and we defer to the committees to share as appropriate. We believe that Congress and law enforcement are best positioned to assess the nature and intent of these activities.

Question 9. What is Facebook doing to limit foreign actors' ability to obtain and use personal information about American users?

Answer. Protecting a global community of more than 2 billion involves a wide range of teams and functions, and our expectation is that those teams will grow across the board. For example, we have dedicated information security and related engineering teams.

Protecting the security of information on Facebook is at the core of how we operate. Security is built into every Facebook product, and we have dedicated teams focused on each aspect of data security. From encryption protocols for data privacy to machine learning for threat detection, Facebook's network is protected by a combination of advanced automated systems and teams with expertise across a wide range of security fields. Our security protections are regularly evaluated and tested by our own internal security experts and independent third parties. For the past seven years, we have also run an open bug bounty program that encourages researchers from around the world to find and responsibly submit security issues to

[5] Young Mie Kim *et al.*, "The Stealth Media? Groups and Targets behind Divisive Issue Campaigns on Facebook," Politcal Communication (forthcoming), available at *https://journalism.wisc.edu/wp-content/blogs.dir/41/files/2018/04/Kim.FB_.StealthMedia.Final_.PolCom.0411181.pdf.*

us so that we can fix them quickly and better protect the people who use our service.

We anticipate continuing to grow these teams by hiring a range of experts, including people with specific types of threat intelligence expertise.

This will never be a solved problem because we're up against determined, creative and well-funded adversaries. But we are making steady progress. Here is a list of the 10 most important changes we have made:

1. Ads transparency. Advertising should be transparent: users should be able to see all the ads an advertiser is currently running on Facebook, Instagram, and Messenger. And for ads with political content, we've created an archive that will hold ads with political content for seven years—including information about ad impressions and spend, as well as demographic data such as age, gender and location. People in Canada and Ireland can already see all the ads that a Page is running on Facebook—and we're launching this globally in June.

2. Verification and labeling. Every advertiser will now need confirm their ID and location before being able to run any ads with political content in the U.S. All ads with political content will also clearly state who paid for them.

3. Updating targeting. We want ads on Facebook to be safe and civil. We thoroughly review the targeting criteria advertisers can use to ensure they are consistent with our principles. As a result, we removed nearly one-third of the targeting segments used by the IRA. We continue to allow some criteria that people may find controversial. But we do see businesses marketing things like historical books, documentaries or television shows using them in legitimate ways.

4. Better technology. Over the past year, we've gotten increasingly better at finding and disabling fake accounts. We now block millions of fake accounts each day as people try to create them—and before they've done any harm. This is thanks to improvements in machine learning and artificial intelligence, which can proactively identify suspicious behavior at a scale that was not possible before—without needing to look at the content itself.

5. Action to tackle fake news. We are working hard to stop the spread of false news. We work with third party fact checking organizations to limit the spread of articles with rated false. To reduce the spread of false news, we remove fake accounts and disrupt economic incentives for traffickers of misinformation. We also use various signals, including feedback from our community, to identify potential false news. In countries where we have partnerships with independent third-party fact-checkers, stories rated as false by those fact-checkers are shown lower in News Feed. If Pages or domains repeatedly create or share misinformation, we significantly reduce their distribution and remove their advertising rights. We also want to empower people to decide for themselves what to read, trust, and share. We promote news literacy and work to inform people with more context. For example, if third-party fact-checkers write articles about a news story, we show them immediately below the story in the Related Articles unit. We also notify people and Page Admins if they try to share a story, or have shared one in the past, that's been determined to be false. In addition to our own efforts, we're learning from academics, scaling our partnerships with third-party fact-checkers and talking to other organizations about how we can work together.

6. Significant investments in security. We're doubling the number of people working on safety and security from 10,000 last year to over 20,000 this year. We expect these investments to impact our profitability. But the safety of people using Facebook needs to come before profit.

7. Industry collaboration. Recently, we joined 34 global tech and security companies in signing a TechAccord pact to help improve security for everyone.

8. Information sharing and reporting channels. In the 2017 German elections, we worked closely with the authorities there, including the Federal Office for Information Security (BSI). This gave them a dedicated reporting channel for security issues related to the Federal elections.

9. Tracking 40+ elections. In recent months, we've started to deploy new tools and teams to proactively identify threats in the run-up to specific elections. We first tested this effort during the Alabama Senate election, and plan to continue these efforts for elections around the globe, including the U.S. midterms. Last year we used public service announcements to help inform people about fake news in 21 separate countries, including in advance of French, Kenyan and German elections.

10. Action against the Russia-based IRA. In April, we removed 70 Facebook and 65 Instagram accounts—as well as 138 Facebook Pages—controlled by the IRA primarily targeted either at people living in Russia or Russian-speakers around the world including from neighboring countries like Azerbaijan, Uzbekistan, and Ukraine. The IRA has repeatedly used complex networks of inauthentic accounts to deceive and manipulate people in the U.S., Europe, and Russia—and we don't want them on Facebook anywhere in the world.

We are taking steps to enhance trust in the authenticity of activity on our platform, including increasing ads transparency, implementing a more robust ads review process, imposing tighter content restrictions, and exploring how to add additional authenticity safeguards.

Question 10. Russian accounts continue to use social media to try to influence American opinion. For example, Fox News started a social media campaign to demand the declassification and release of the Nunes memo, which attacked the FBI's Russia investigation. Within hours, Russian bots were promoting the release of the memo.

a. When this began did Facebook investigate whether Russians were using its platforms to promote the "Release the Memo" campaign?

b. Has Facebook analyzed whether any of the accounts that users shared WikiLeaks' offer of $1 million for a copy of the Nunes memo (before it was declassified and released) had connections to Russian-backed accounts?

Answer. As of our February 7, 2018 letter to you on this issue, our internal Information Security team has not become aware of information or activity of a sort that would prompt further review. In addition to reaching out to law enforcement and our industry partners to understand whether they have any relevant information regarding this issue and Russian influence more generally, our Information Security team regularly conducts internal reviews to monitor for state-sponsored threats. While we do not publicly disclose the elements of these reviews for security reasons, factors include monitoring and assessing thousands of detailed account attributes, such as location information and connections to others on our platform. We are committed to keeping law enforcement apprised of our efforts and to working together to address this threat.

Question 11. How many communications has Facebook had with individuals associated with any accounts that Facebook has identified as Internet Research Agency accounts?

Answer. Last fall, we concluded that sharing the ads we've discovered with Congress, in a manner that is consistent with our obligations to protect user information, will help government authorities complete the vitally important work of assessing what happened in the 2016 election. That is an assessment that can be made only by investigators with access to classified intelligence and information from all relevant companies and industries—and we want to do our part. Congress is best placed to use the information we and others provide to inform the public comprehensively and completely. Our practice is to provide messages in response to valid legal process. The ads (along with the targeting information) are publicly available at *https://democrats-intelligence.house.gov/facebook-ads/social-media-advertisements.htm*.

Question 12. On October 27, 2017, I asked you to provide to the Committee all communications between Facebook and individuals or entities associated with Russia-connected users that posted ads or organic content targeted to any part of the United States for the time period from January 2, 2015 to the date of production. You have not yet provided a substantive response to this request. Please provide these communications.

Answer. See Response to Question 11.

Question 13. Please provide all organic Instagram posts for Internet Research Agency accounts that targeted users in the United States.

Answer. Facebook provided all of these posts to the Senate Judiciary Committee last fall on October 30 and 31.

Global Privacy Protections

Question 14. You have said that Facebook would apply the European Union's new privacy requirements globally in spirit.

a. Will the privacy requirements be incorporated into the terms of service that apply to users in the United States? If not, why not? If so, when will this change be made?

b. It was recently reported that Facebook users outside of the United States and Canada had previously been governed by terms of service agreed with Facebook in

Ireland.[6] Facebook is apparently changing this so that non-European Union users will have their terms of service agreed with Facebook in the United States. This affects 1.5 billion users. Does this mean that the European Union's new privacy requirements will not apply to these 1.5 billion users? If Facebook intends to provide the same privacy protections and controls to users globally, why did it make this change?

Answer. The change referred to in this question involves the legal entity with which Facebook users contract when they use the service, which changed in some jurisdictions as a part of the most recent updates to our Terms of Service and Data Policy. This change did not impact people who live in the United States, who contract with Facebook, Inc. under both our new and old policies.

The substantive protections in our user agreements offered by Facebook Ireland and Facebook, Inc. are the same. However, there are certain aspects of our Facebook Ireland Data Policy that are specific to legal requirements in the GDPR—such as the requirement that we provide contact information for our EU Data Protection Officer (DPO) or that we identify the "legal bases" we use for processing data under the GDPR. Likewise, our Facebook Ireland terms and Data Policy address the lawful basis for transferring data outside the EU, based on legal instruments that are applicable only to the EU.

In any case, the controls and settings that Facebook is enabling as part of GDPR are available to people around the world, including settings for controlling our use of face recognition on Facebook and for controlling our ability to use data we collect off Facebook Company Products to target ads. We recently began providing direct notice of these controls and our updated terms to people around the world (including in the U.S.), allowing people to choose whether or not to enable or disable these settings or to consent to our updated terms. We provide the same tools for access, rectification, erasure, data portability, and others to people in the U.S. and rest of world that we provide in Europe, and many of those tools (like our Download Your Information tool, ad preferences tool, and Activity Log) have been available globally for many years.

We are also looking to be more responsive to regional norms and legal frameworks going forward, and want to have the flexibility to work with local regulators, which is possible with this new model. At the same time, we are changing the provisions in our Facebook, Inc. terms in our user agreements outside the United States to allow people in other countries to file lawsuits against Facebook in their home country, rather than in courts in the U.S. This transition was part of a continued effort to be locally responsive in countries where people use our services.

RESPONSE TO WRITTEN QUESTIONS SUBMITTED BY HON. PATRICK LEAHY TO MARK ZUCKERBERG

Question 1. At the April 10, 2018 hearing, regarding Facebook's role in facilitating dangerous hate speech against Rohingya refugees from Myanmar, I asked: "How can you dedicate, and will you dedicate, resources to make sure such hate speech is taken down within 24 hours?"

You replied, "Yes. We're working on this."[7] I appreciate your commitment, in the context of Myanmar, to dedicate resources to take down hate speech within 24 hours. As you know, hours can save lives.

a. When will Facebook be able to fully implement your commitment to a 24-hour review time for Myanmar?

i. Will Facebook commit to providing relevant data so that outside researchers can evaluate Facebook's performance metrics on this matter?

b. Will you extend this same commitment to dedicating the resources necessary to achieve a 24-hour review time for hate speech in all other regions of the world in which Facebook is active?

Answer. Reports are reviewed 24 hours a day, 7 days a week, and the vast majority of reports are reviewed within 24 hours. Where there are credible threats of violence we aim to respond much faster, and have significantly reduced our response time in Myanmar.

To support these efforts, we are investing in people, technology, and programs.

Over the last two years, we have added dozens more Burmese language reviewers to handle reports from users across our services, and we plan to more than double

---

[6] Alex Hern, "Facebook moves 1.5bn users out of reach of new European privacy law," The Guardian (Apr. 19, 2018).

[7] Transcript of April 10, 2018 hearing, at *https://www.washingtonpost.com/news/the-switch/wp/2018/04/10/transcript-of-mark-zuckerbergs-senate-hearing/?utm_term=.5789208de46b*.

the number of content reviewers focused on user reports. We also have increased the number of people across the company working on Myanmar-related issues and we have a special product team working to better understand the local challenges and build the right tools to help keep people in the country safe. We will continue to hire more staff dedicated to Myanmar, including Burmese speakers and policy experts.

From a programmatic perspective, we will continue to work with experts to develop safety resources and counter-speech campaigns in these regions and conduct regular training for civil society and community groups on using our tools.

Question 2. At the hearing, I showed you an example of a Facebook post targeting a Muslim journalist in Myanmar. Although comments to the incendiary post called for the death of this journalist, upon an initial review the post was deemed not to breach Facebook's Community Standards.

a. Why was this post deemed not to breach Facebook's Community Standards?

b. Please describe what processes and systems you have in place to proactively identify content that breaches Facebook's Community Standards.

c. What emergency processes do you have in place for situations where there is content inciting people to violence, and that content has been reported by users and deemed not to breach your Community Standards?

d. Please describe any additional processes that you intend to put in place to address this problem in the future.

We are unable to respond without further information on these Pages.

However, we can say that our Community Standards strictly prohibit credible threats of violence. We assess credibility based upon the information available to us and generally consider statements credible if the following are present:

- A target (person, group of people, or place) and:
  - Bounty/demand for payment, or
  - Mention or image of specific weapon, or o Sales offer or ask to purchase weapon, or o Spelled-out address or named building, or
- A target and two or more of the following details (can be two of the same detail):
  - Location
  - Timing
  - Method

In evaluating content, context is extremely important. A post itself may be benign, but the comments associated with the post may amount to credible threats of violence. That's why people can report posts, Pages, and Groups to us, as well as individual comments.

The other way we can identify and remove violating content from Facebook is by proactively finding it using technology. Advances in technology, including in artificial intelligence, machine learning, and computer vision, mean that we can now:

- *Remove bad content faster* because we don't always have to wait for it to be reported.
- *Get to more content* because we don't have to wait for someone else to find it.
- *Increase the capacity of our review team*, which includes more than 7,500 people around the world, to work on cases where human expertise is needed to understand the context or nuance of a particular situation.

Question 3. At the hearing, you stated that Facebook is hiring "dozens more" Burmese language content reviewers. There appear to be only three Burmese content reviewer vacancies currently listed on the Facebook careers page, all in Facebook's Dublin office.[8]

a. How many Myanmar (Burmese) content reviewers does Facebook currently have, and how many does Facebook expect to have on staff by the end of 2018? Please use Full Time Equivalent (FTE) numbers.

b. How does Facebook staff its Burmese language content reviewers to ensure the capacity to promptly review content outside of normal Dublin working hours, including during daytime and on weekends in the Myanmar time zone? How many Burmese language content reviewers do you have based in Southeast Asia?

[8] *See https://www.facebook.com/careers/.*

c. Facebook reportedly has approximately 1,200 German language content reviewers, in part to help ensure that hate speech is removed within 24 hours. How are "dozens" of Burmese content reviewers going to be sufficient to remove all Burmese language hate speech within 24 hours?

Answer. To provide 24/7 coverage across dozens of languages and time zones and ensure that Facebook is a place where both expression and personal safety are protected and respected, our content review teams are made up of a combination of full-time employees, contractors, and vendor partners based in locations around the world.

Our content review team has included Burmese language reviewers since 2013, and we have increased this number over time as we continue to grow and invest in Myanmar. Our goal is always to have the right number of people with the native language capabilities to ensure incoming reports are reviewed quickly and effectively.

Reports are reviewed 24 hours a day, 7 days a week and the vast majority of reports are reviewed within 24 hours. Where there are credible threats of violence we aim to respond much faster, and have significantly reduced our response time in Myanmar.

That said, there is more to tackling this problem than reported content. A lot of abuse may go unreported, which is why we are exploring the use of artificial intelligence to proactively identify this content so that we can find it and review it faster.

Question 4. Facebook has long stated its desire to re-enter the market in China.[9] As we have seen with other technology platforms, however, there is a cost to doing business in China, including potentially enabling the Chinese government's sophisticated censorship and surveillance regimes. I expressed these concerns to Apple in a letter with Senator Cruz last year.[10]

a. In order to operate in China, Internet companies must generally comply with Chinese laws and regulations on censorship.[11] This includes a requirement to remove content relating to a list of vaguely-defined prohibited topics such as "disrupting social order and stability" or "damaging state honor and interests."[12] Given the vagueness surrounding which precise words and terms are prohibited in China, how would Facebook decide what specific content to censor in China? And if a China-based user travels outside of China, will those censorship controls still apply to that user's account?

Answer. Because Facebook has been blocked in China since 2009, we are not in a position to know exactly how the government would seek to apply its laws and regulations on content were we permitted to offer our service to Chinese users. Since 2013, Facebook has been a member of the Global Network Initiative (GNI), a multi-stakeholder digital rights initiative. As part of our membership, Facebook has committed to the freedom of expression and privacy standards set out in the GNI Principles—which are in turn based on the Universal Declaration of Human Rights and the United Nations Guiding Principles on Business and Human Rights—and we are independently assessed on our compliance with these standards on a biennial basis.

b. According to *The New York Times,* Facebook developed "software to suppress posts from appearing in people's news feeds in specific geographic areas," in order to "help Facebook get into China."[13] If true, then what procedures did such software assume would be used to identify specific content to censor, given the vagueness surrounding prohibited topics under Chinese law?

Answer. See Response to Question 4a.

c. Under domestic Chinese law, peaceful acts of free expression may be considered illegal. For example, the Chinese government has described the late Nobel Peace laureate Liu Xiaobo as "a criminal who has been sentenced by Chinese judicial de-

---

[9] *See, e.g.,* Answers to Questions for the Record by Colin Stretch, submitted to the Subcommittee on Crime and Terrorism, Oct. 31, 2017, at *https://www.judiciary.senate.gov/download/stretch-responses-to-questions-for-the-record.*

[10] *See https://www.cruz.senate.gov/files/documents/Letters/20171017_tim_cook_letter.pdf.*

[11] "China Has Launched Another Crackdown on the Internet—but it's Different This Time", CNBC, Oct. 26, 2017, at *https://www.cnbc.com/2017/10/26/china-internet-censorship-new-crackdowns-and-rules-are-here-to-stay.html. See also,* "Media Censorship in China," COUNCIL ON FOREIGN RELATIONS, at *https://www.cfr.org/backgrounder/media-censorship-china.*

[12] *See https://citizenlab.ca/2016/11/wechat-china-censorship-one-app-two-systems/.*

[13] "Facebook Said to Create Censorship Tool to Get Back Into China," THE NEW YORK TIMES, Nov. 22, 2016, at *https://www.nytimes.com/2016/11/22/technology/facebook-censorship-tool-china.html.*

partments for violating Chinese law."[14] The case of Tashi Wangchuk indicates that simply promoting the Tibetan language can be deemed illegally "inciting separatism."[15] If Facebook re-enters the Chinese market, what would it do if Chinese authorities serve it with a legal demand, properly issued under domestic Chinese law, asking Facebook to turn over the account information of a peaceful political or religious dissident in China?

Answer. When something on Facebook or Instagram is reported to us as violating local law, but doesn't go against our Community Standards, we may restrict the content's availability only in the country where it is alleged to be illegal after careful legal review. We receive reports from governments and courts, as well from non-government entities such as members of the Facebook community and NGOs. Because Facebook has been blocked in China since 2009, we are not in a position to know exactly how the government would seek to apply its laws and regulations were we permitted to offer our service to Chinese users. Wherever we operate our service, Facebook is committed to meeting human rights' standards and to providing transparency around any government requests for data. This information is available here: *https://transparency.facebook.com/content-restrictions*. Our Transparency Report contains data on restrictions we place on content that does not violate community standards but that is alleged to violate local law. We do not have any such reports for the United States.

Question 5. On April 9, 2018, a group of Vietnamese activists and journalists wrote to you to ask whether Facebook was "coordinating with a government known for cracking down on expression."[16]

a. What safeguards does Facebook have in place to ensure that account suspension and content takedown are not abused by governments—including in conjunction with state-sponsored "trolls"—to silence legitimate criticism?

Answer. As a GNI member, Facebook is committed to privacy and free expression principles and implementation guidelines regarding government requests. The GNI standards have been shaped by international human rights laws and norms and developed through a robust multi-stakeholder and consultative process.

b. What more can and will Facebook do in this regard, including but not limited to providing more transparency and more accessible appeal mechanisms on takedown decisions?

Answer. On April 24, 2018, we published the internal guidelines we use to enforce our Community Standards. We decided to publish these internal guidelines for two reasons. First, the guidelines will help people understand where we draw the line on nuanced issues. Second, providing these details makes it easier for everyone, including experts in different fields, to give us feedback so that we can improve the guidelines—and the decisions we make—over time.

We know we need to do more. That's why, over the coming year, we are going to build out the ability for people to appeal our decisions. As a first step, we are launching appeals for posts that were removed for nudity/sexual activity, hate speech or graphic violence.

Here's how it works:

- If a user's photo, video, or post has been removed because we found that it violates our Community Standards, they will be notified, and given the option to request additional review.
- This will lead to a review by our team (always by a person), typically within 24 hours.
- If we've made a mistake, we will notify the user and their post, photo or video will be restored.

We are working to extend this process further, by supporting review of more violation types, giving people the opportunity to provide more context that could help us make the right decision, and making appeals available not just for content that was taken down, but also for content that was reported and left up. We believe giving

---

[14] "Nobel Peace Prize Given to Jailed Chinese Dissident," THE NEW YORK TIMES, Oct. 8, 2010, at *https://www.nytimes.com/2010/10/09/world/09nobel.html?pagewanted=all*.

[15] "China to Try Tibetan Education Advocate Detained for 2 Years," THE NEW YORK TIMES, Dec. 30, 2017, at *https://www.nytimes.com/2017/12/30/world/asia/tashi-wangchuck-trial-tibet.html*.

[16] *See http://viettan.org/en/open-letter-to-facebook/*. See also, "Vietnam Activists Question Facebook on Suppressing Dissent," REUTERS, April 10, 2018, at *https://www.reuters.com/article/us-facebook-privacy-vietnam/vietnam-activists-question-facebook-on-suppressing-dissent-idUSKBN1HH0DO*.

people a voice in the process is another essential component of building a fair system.

Question 6. Like so many other companies, Facebook has made promises before to do better on privacy, including in its consent decree with the FTC. But the American people want accountability, not promises. That is why I introduced my Consumer Privacy Protection Act, which would create standards and require prompt notification when a breach occurs. It is important to note that we only know about the Cambridge Analytica breach because of a whistleblower.

a. Facebook did not notify the 87 million users when it learned of this breach in 2015, but you are doing so now. You have now said that Facebook's failure to notify 87 million users that their information had been compromised in the Cambridge Analytica breach was a "mistake." Would you support legislation requiring prompt notification of data breaches (with appropriate temporary exceptions for ongoing investigations, law enforcement, and national security)?

b. Why did Facebook not verify that Cambridge Analytica actually deleted the data—especially in 2016 when it was known they were working for the Trump campaign?

Answer. Facebook is generally open to the idea of breach notification requirements, particularly legislation that would centralize reporting and ensure a consistent approach across the United States. For example, in Europe, the GDPR requires notification to a lead supervisory authority, rather than individual member states, in cases of a data breach. In the United States, however, there is no centralized notification scheme, and instead, reporting obligations vary widely across all 50 states. This complexity makes it harder to respond appropriately and swiftly to protect people in the event of a data breach. We believe this is an important issue and an area that is ripe for thoughtful regulation.

When Facebook learned about Kogan's breach of Facebook's data use policies in December 2015, it took immediate action. The company retained an outside firm to assist in investigating Kogan's actions, to demand that Kogan and each party he had shared data with delete the data and any derivatives of the data, and to obtain certifications that they had done so. Because Kogan's app could no longer obtain access to most categories of data due to changes in Facebook's platform, the company's highest priority at that time was ensuring deletion of the data that Kogan may have accessed before these changes took place. With the benefit of hindsight, we wish we had notified people whose information may have been impacted. Facebook has since notified all people potentially impacted with a detailed notice at the top of their News Feed.

Question 7. In a recent interview, Dr. Aleksandr Kogan described an extensive relationship with Facebook, stating that "I visited their campus many times. They had hired my students. I even did a consulting project with Facebook in November of 2015." According to *60 Minutes,* Facebook confirmed that Kogan had done research and consulting with the company in 2013 and 2015.[17] Please detail Facebook's relationship with Dr. Kogan, including any consulting and research he did for the company. Please describe what, if any, access to user data Dr. Kogan and his company was provided as part of this consulting agreement.

Answer. Facebook was put in touch with Kogan (a researcher at the University of Cambridge) in late 2012, about a possible collaboration on research relating to the potential relationship between Facebook friendship ties and economic trade volumes between countries. Kogan collaborated with current and former Facebook employees on approximately ten academic papers. As part of these collaborations, Kogan could only access fully anonymized, aggregated data. Facebook frequently partners with leading academic researchers to address topics pertaining to wellbeing, innovation, and other topics of public importance, following strict protocols to ensure personal information is safeguarded.

In October 2015, Facebook retained Kogan on a short-term contract to consult on a research project related to predicting survey outcomes.

Question 8. In 2010, media reports revealed that that an online tracking company, RapLeaf, was collecting and reselling data it had obtained from third-party Facebook apps. Facebook subsequently reportedly cut off RapLeaf's data access and took steps to limit apps' sharing of data with the company.[18]

---

[17] *See https://www.cbsnews.com/news/aleksandr-kogan-the-link-between-cambridge-analytica-and-facebook/.*

[18] *See, e.g., http://www.adweek.com/digital/facebook-shuts-down-apps-that-sold-user-data-bans-rapleaf/* and *https://www.wsj.com/articles/SB10001424052702304772804575558484075236968.*

a. Please describe what steps, if any, Facebook took to require RapLeaf to delete the Facebook user data it had obtained, and the subsequent steps Facebook took to ensure that the information was in fact deleted. If Facebook did not act to ensure that RapLeaf deleted this data, please describe why.

b. Please describe what steps, if any, Facebook took with respect to any third party apps that had sold or shared Facebook user data with RapLeaf.

Answer. Facebook disabled all RapLeaf domains and instituted six-month moratoriums on access to Facebook distribution channels for the developers who shared data. RapLeaf agreed to delete all Facebook IDs in its possession, immediately terminate all agreements with Facebook developers, and no longer conduct any activity on the Facebook platform, whether directly or indirectly. Facebook updated its terms of service to explicitly prohibit developers from interacting with any data brokers.

Question 9. At the hearing, you stated "every single time they choose to share something, there [on Facebook]—they have a control right there about who they want to share it with."[19] If a user sets these privacy controls to limit their information to a specific audience (*e.g.* their "friends"), should that user expect that no other parties—including Facebook's advertising algorithms—will be able to view or use that information? Should this expectation extend to the trail of information that the user generates by interacting with the service (*e.g.,* "likes" and other reactions, IP logins, geolocation, and operating system usage)?

Answer. Our goal is to show people information on Facebook that's relevant and useful to them. To do this, we personalize people's news feeds and other information, including ads, that we show them based on the information that they've added to their Facebook accounts, like the things they like or comment on.

People can control how this works through their News Feed Settings and Ad Preferences, and they can also choose who can see the information that they choose to share on Facebook. With regard to advertisers specifically, though, we do not tell advertisers who people are or sell their information to anyone. We think relevant advertising and privacy aren't in conflict, and we're committed to doing both well.

Question 10. Beyond information provided directly in response to valid legal process in individual criminal matters, does Facebook provide any information about users to, or cooperate in any way with, Federal, State, or local agencies or authorities—or companies working on their behalf—in a way that would allow for user profiling and/or predictive analytics?

Answer. Facebook is not familiar with government agencies' practices regarding profiling and/or predictive analytics and therefore cannot speculate what would "allow for" such agencies to use such techniques. Facebook discloses account records to Federal, State, or local agencies and authorities only in accordance with our terms of service and applicable law. Additionally, we prohibit developers from using data obtained from us to provide tools that are used for surveillance.

Question 11. One critique of social media in general is that the most sensational or provocative material often tends to spread the fastest, due to algorithms that prioritize "engagement." This can contribute to a deepening polarization of society. What is Facebook doing with regards to its algorithms, if anything, to address this problem? And what role to you see for outside auditing, verification, or checks of these solutions, given the impact on society?

Answer. Facebook is a distribution platform that reflects the conversations, including polarized ones, already taking place in society. We are keenly aware of the concern that our platform is contributing to polarization, and we have been working to understand the role that we play in discourse and information diversity. The data on what causes polarization and "filter bubbles" is mixed. Some independent research has shown that social media platforms provide more information diversity than traditional media, and our own research indicates that most people on Facebook have at least some friends who claim an opposing political ideology—probably because Facebook helps people to maintain ties with people who are more distantly connected to them than their core community—and that the content in News Feed reflects that added diversity.

We want Facebook to be a place where people can discover more news, information, and perspectives, and we are working to build products that help to that. Through our News Feed algorithm, we also work hard to actively reduce the distribution of clickbait, sensationalism, and misinformation, on the one hand, and to boost news and information from sources that are trusted, informative, and local, on the other hand.

---

[19] Transcript of April 10, 2018 hearing, at *https://www.washingtonpost.com/news/the-switch/wp/2018/04/10/transcript-of-mark-zuckerbergs-senate-hearing/?utm_term=.5789208de46b.*

Question 12. Some people have claimed that what Cambridge Analytica did was no different than the Obama campaign's data-driven campaign in 2012.

a. Yes or no, did the Obama campaign in 2012 violate any of Facebook's policies, and thereby get banned from the platform?

Answer. Both the Obama and Romney campaigns had access to the same tools, and no campaign received any special treatment from Facebook.

b. Yes or no, did Cambridge Analytica violate multiple policies—including misleading users and Facebook, and improperly exploiting user data—and thereby get banned from your platform?

Answer. By passing information on to a third party, including SCL/Cambridge Analytica and Christopher Wylie of Eunoia Technologies, Kogan violated our platform policies. When we learned of this violation in 2015, we removed his app from Facebook and demanded certifications from Kogan and all parties he had given data to that the information had been destroyed. Cambridge Analytica, Kogan, and Wylie all certified to us that they destroyed the data. In March 2018, we received reports that, contrary to the certifications we were given, not all data was deleted. We are moving aggressively to determine the accuracy of these claims. If true, this is another unacceptable violation of trust and the commitments they made. We have suspended SCL/Cambridge Analytica, Wylie, and Kogan from Facebook, pending further information.

RESPONSE TO WRITTEN QUESTIONS SUBMITTED BY HON. RICHARD DURBIN TO MARK ZUCKERBERG

For questions with subparts, please answer each subpart separately.

Question 1. Mr. Zuckerberg, at your hearing I asked whether it is fair for users of Facebook to expect to know what information Facebook is collecting on them, who Facebook is sending the information to, and whether Facebook asked the user in advance for permission to do that. You answered "yes" and said "I think everyone should have control over how their information is used."

a. In order for users to know what information Facebook is collecting on them, will Facebook commit to proactively notifying each Facebook user via e-mail on at least an annual basis that the user can securely view all information that Facebook has collected on that user during the previous year and providing the user with instructions for how to do so?

Answer. Our Download Your Information or "DYI" tool is Facebook's data portability tool and was launched many years ago to let people access and download many types of information that we maintain about them. The data in DYI and in our Ads Preferences tool contain each of the interest categories that are used to show people ads, along with information about the advertisers are currently running ads based on their use of an advertiser's website or app. People also can choose not to see ads from those advertisers. We recently announced expansions to Download Your Information, which, among other things, will make it easier for people to see their data, delete it, and easily download and export it. More information is available at *https://newsroom.fb.com/news/2018/04/new-privacy-protections*.

Responding to feedback that we should do more to provide information about websites and apps that send us information when people use them, we also announced plans to build Clear History. This new feature will enable users to see the websites and apps that send us information when they use them, delete this information from their account, and turn off Facebook's ability to store it associated with their account going forward.

We have also introduced Access Your Information. This feature provides a new way for people to access and manage their information. Users can go here to delete anything from their timeline or profile that they no longer want on Facebook. They can also see their ad interests, as well as information about ads they've clicked on and advertisers who have provided us with information about them that influence the ads they see. From here, they can go to their ad settings to manage how this data is used to show them ads.

b. Will Facebook commit to proactively notifying each Facebook user via e-mail on at least an annual basis that the user can securely view a list of all entities to which Facebook has sent any of the user's information during the previous year and providing the user with instructions on how to do so?

Answer. Facebook allows people to view, manage, and remove the apps that they have logged into with Facebook through the App Dashboard. We recently prompted everyone to review their App Dashboard as a part of a Privacy Checkup, and we also provided an educational notice on Facebook to encourage people to review their

settings. More information about how users can manage their app settings is available at *https://www.facebook.com/help/218345114850283?helpref=about_content*.

The categories of information that an app can access are clearly disclosed before the user consents to use an app on the Facebook Platform. Users can view and edit the categories of information that apps they have used have access to through the App Dashboard.

Question 2. At your hearing, I pointed out that information is collected on users by Facebook and "sometimes, people have made money off of sharing that information" without the users' knowledge or advance consent. You responded by saying you would provide information about Facebook's developer platform, and I asked if you could provide that information for the record because of limited time. Please provide this information for the record.

Answer. In 2007, there was industry-wide interest in enriching and expanding users' experiences on various platforms by allowing them to take their data (from a device or service) to third-party developers to receive new experiences. For example, around that time, Apple and Google respectively launched their iOS and Android platforms, which were quickly followed by platform technologies and APIs that allowed developers to develop applications for those two platforms and distribute them to users through a variety of channels. Similarly, in 2007, Facebook launched a set of platform technologies that allowed third parties to build applications that could run on and integrate with the Facebook service and that could be installed by Facebook users who chose to do so. In December 2009, Facebook launched new privacy controls that enabled users to control which of the types of information that they made available to their friends could be accessed by apps used by those friends.

As with all of these platforms, the permissions model that governed the information that third-party applications could access from the Platform evolved. For example, in April 2010, Facebook launched granular data permissions (GDP), which allowed users to examine a list of categories of information that an app sought permission to access before they authorized the app.

Throughout the relevant period and through today, Facebook's policies regarding third-party usage of its platform technologies have prohibited—and continue to prohibit—those third-party app developers from selling or licensing user data obtained from Facebook or from sharing any user data obtained from Facebook with any ad network, data broker or other advertising or monetization-related service.

In November 2013, when Kogan launched the app, apps generally could be launched on the Platform without affirmative review or approval by Facebook. The app used the Facebook Login service, which allowed users to utilize their Facebook credentials to authenticate themselves to third-party services. Facebook Login and Facebook's Graph API also allowed the app to request permission from its users to bring their Facebook data (their own data and data shared with them by their friends) to the app, to obtain new experiences.

At that time, the Graph API V1 allowed app developers to request consent to access information from the installing user such as name, gender, birthdate, location (*i.e.,* current city or hometown), photos and Page likes—and also (depending on, and in accordance with, each friend's own privacy settings) the same or similar categories of information the user's friends had shared with the installing user. Permitting users to share data made available to them by their friends had the upside of making the experience of app users more personalized and social. For example, a Facebook user might want to use a music app that allowed the user to (1) see what his or her friends were listening to and (2) give the app permission to access the user's friend list and thereby know which of the user's friends were also using the app. Such access to information about an app user's friends required not only the consent of the app user, but also required that the friends whose data would be accessed have their own privacy settings set to permit such access by third-party apps. In other words, Kogan's app could have accessed a user's friends' information only for friends whose privacy settings permitted such sharing.

In April 2014, we announced that we would more tightly restrict our platform APIs to prevent abuse. At that time we made clear that existing apps would have a year to transition—at which point they would be forced (1) to migrate to the more restricted API and (2) be subject to Facebook's new review and approval protocols. A small number of developers asked for and were granted short-term extensions beyond the one-year transition period, the longest of which lasted several months. These extensions ended several years ago. A transition period of this kind is standard when platforms implement significant changes to their technology base and was necessary here to avoid disrupting the experience of millions of people. New apps that launched after April 30, 2014 were required to use our more restrictive platform APIs, which incorporated several key new elements, including:

- Institution of a review and approval process, called App Review (also called Login Review), for any app seeking to operate on the new platform that would request access to data beyond the user's own public profile, e-mail address, and a list of friends of the user who had installed and authorized the same app;
- Generally preventing new apps on the new platform from accessing friends data without review; and
- Providing users with even more granular controls over their permissions as to what categories of their data an app operating on the new platform could access.

Our investigation is ongoing and as part of it we are taking a close look at applications that had access to friends data under Graph API v.1.0 before we made technical changes to our platform to change this access.

The App Review process introduced in 2014 required developers who create an app that asks for more than certain basic user information to justify the data they are looking to collect and how they are going to use it. Facebook then reviewed whether the developer has a legitimate need for the data in light of how the app functions. Only if approved following such review can the app ask for a user's permission to get their data. Facebook has rejected more than half of the apps submitted for App Review between April 2014 and April 2018, including Kogan's second app. We are changing Login so that the only data that an app can request without app review will include name, profile photo, and e-mail address.

Question 3. At your hearing I asked you about Messenger Kids and asked "what guarantees can you give us that no data from Messenger Kids is or will be collected or shared" in ways that might violate the Children's Online Privacy Protection Act. You said "in general, that data is not going to be shared with third parties." I noted that your use of the qualifier "in general" "seems to suggest that in some circumstances it will be shared with third parties" You responded "no, it will not."

a. Please describe any information collected via Messenger Kids that is shared by Facebook with any third party.

Answer. We have no plans to include advertising in Messenger Kids. Moreover, there are no in-app purchases, and we do not use the data in Messenger Kids to advertise to children or their parents. In developing the app we assembled a committee of advisors, including experts in child development, online safety, and media and children's health, and we continue to work with them on an ongoing basis. In addition, we conducted roundtables with parents from around the country to ensure we were addressing their concerns and built the controls they need and want in the app. We are committed to approaching all efforts related to children 12 and under thoughtfully, and with the guidance and input of experts and parents.

b. Please confirm for the record that no data collected from Messenger Kids is, or will be, shared with third parties in violation of COPPA.

Answer. See Response to Question 3a.

Question 4. At your hearing, I asked "would you be open to the idea that someone having reached adult age having grown up with Messenger Kids be allowed to delete the data you have collected?" You said "Senator, yes . . . I think it is a good idea to consider making sure that all that information is deleted."

a. Will you commit to allow children, when they reach adulthood, to request that any information gathered about them by Facebook while they were under age 13 be deleted and will you commit that Facebook will comply with such requests?

b. Do you support giving American Internet users the ability to request the deletion of any and all information collected as a result of a user's online activities prior to age 13, and to require companies to delete such information when an individual has requested it?

c. Do you think children would benefit from the ability to wipe clean the information that has been gathered and collected on them through their online activities before age 13?

d. Do children deserve the chance to grow up and learn how to responsibly use the Internet prior to age 13 without having their childhood Internet data preserved in perpetuity by for-profit companies?

Answer. Under our Messenger Kids Privacy Policy, available at *https://www.facebook.com/legal/messengerkids/privacypolicy*, Parents can control their children's accounts. Through the Parent Dashboard in their Facebook (or Messenger) account, a parent or guardian can review and edit their child's Messenger Kids profile information, and remove contacts to prevent further communication with their child on Messenger Kids. In addition, a parent or guardian who has authorized the Messenger Kids app can see their child's interactions on Messenger

Kids by accessing their child's account. In order to stop further collection and use of their child's personal information on Messenger Kids, a parent or guardian can delete their child's Messenger Kids account. If a parent deletes their child's account, Facebook deletes their Messenger Kids registration information, information about their activity and contacts, and device information, as described above. However, the messages and content a child sent to and received from others before their account was deleted may remain visible to those users.

Question 5. What do you think is the maximum amount of time per day that a child under age 13 should spend using Internet social media?

Answer. We are committed to working with parents and families, as well as experts in child development, online safety and children's health and media, to ensure we are building better products for families—that means building tools that promote meaningful interactions and help people manage their time on our platform and it means giving parents the information, resources and tools they need to set parameters for their children's use of online technologies and help them develop healthy and safe online habits. It also means continued research in this area.

Indeed, Messenger Kids, the only product we offer to children under the age of 13, includes Sleep Mode, which gives parents the ability to set parameters on when the app can be used, and the app does not have ads or in app purchases. In building the app, we worked closely with leading child development experts, educators, and parents to inform our decisions and we continue to work with them on an ongoing basis. Our advisors included experts in the fields of child development, online safety and children's media currently and formerly from organizations such as the Yale Center for Emotional Intelligence (*http://ei.yale.edu/who-we-are/mission/*), Connect Safely (*http://www.connectsafely.org/about-us/*), Center on Media and Child Health (*http://cmch.tv/*), Sesame Workshop (*http://www.huffingtonpost.com/author/dr-lewis-bernstein*) and more.

We also have a Parents Portal (*https://www.facebook.com/safety/parents*) and Youth Portal (*https://www.facebook.com/safety/youth*), which are both focused on fostering conversations around online safety, security, and well-being and giving parents and young people access to the information and resources they need to make informed decisions about their use of online technologies.

Question 6. Does Facebook agree that states have a strong interest in protecting the privacy of their residents?

Answer. We believe strongly in providing meaningful privacy protections to people. This is why we work hard to communicate with people about privacy and build controls that make it easier for people to control their information on Facebook. For example, Facebook has redesigned its settings menu to make things easier to find and introduced new Privacy Shortcuts. These shortcuts allow users to make their account more secure, control their personal information, control which ads they see, and control who sees their posts and profile information. Facebook has also introduced additional tools to find, download, and delete user data.

We've worked with regulators, legislators, and privacy experts, at both the state and national levels to educate people and businesses about privacy. We believe an important component of any privacy regulation is clear and consistent oversight and enforcement. We intend to continue this collaborative work to promote privacy protections for our community.

Question 7. Does Facebook think companies should have to get Americans' consent before scanning and storing their biometric data?

Answer. Facebook uses facial recognition technology to provide people with products and features that enhance online experiences for Facebook users while giving them control over this technology. Facebook's facial recognition technology helps people tag their friends in photos; gives people an easier and faster way to privately share their photos with friends; helps people with visual impairments by generating descriptions of photos that people using screen readers can hear as they browse Facebook; lets people know when a photo or video of them has been uploaded to Facebook, even if they are not tagged; and helps prevent people from impersonating other Facebook users.

Facial recognition technology uses machine-learning algorithms to analyze the pixels in photos and videos in which a user is tagged, and the photo used by the person as his or her profile picture, and generates a unique number called a template. When a photo or video is uploaded to Facebook, Facebook uses the template to attempt to identify someone by determining whether there are any faces in that content, and analyzing the portion of the image in which the face appears to compare it against certain Facebook users depending on the purpose for which facial recognition is being performed.

Facebook has not shared and does not have plans to share or make available to any third party its facial recognition templates. Moreover, these templates do not provide meaningful information on their own; they can be used to identify a person only in conjunction with Facebook's software. They could not be reverse-engineered to recreate someone's face.

Facebook designed its facial-recognition technology and the applications that use it with privacy considerations in mind and incorporated various safeguards and controls that protect both (1) users' ability to control the collection, use, and disclosure of their personal information, and (2) the security of that personal information.

Facebook gives users control over whether Facebook uses facial recognition to recognize them in photos and videos. That control is exercised through users' privacy settings. If a user chooses to turn facial recognition off, Facebook does not create a template for that person or deletes any template it has previously created. Facebook will then be unable to recognize that person in any photos or videos that are uploaded to the service. Facebook also deletes templates of people who delete their Facebook accounts. Additionally, Facebook does not maintain templates for users who have no photos tagged of themselves and do not have a profile photo that is capable of being used to generate a face signature or template (*e.g.,* where a user has no profile photo, where a user's profile photo does not contain a human face, or where a user's profile photo contains multiple untagged faces).

We inform people about our use of facial-recognition technology through the Data Policy, Help Center, posts on Facebook, and direct user notifications. Facebook users are told that they can opt out of facial recognition at any time—in which case Facebook will delete their template and will no longer use facial recognition to identify them.

In creating facial recognition templates, Facebook uses only data that people have voluntarily provided to Facebook: the photos and videos that people have voluntarily uploaded to Facebook (including public profile pictures) and the tags people have applied to those photos and videos. Facebook does not use facial recognition to identify someone to a stranger.

Question 8. Has Facebook advocated for any changes to the Illinois Biometric Information Privacy Act, either on its own or as the member of a trade association or state chamber of commerce?

Answer. We are aware of several pending measures to amend the Illinois Biometric Information Privacy Act to foster the use of technology to enhance privacy and data security and combat threats like fraud, identity theft, and impersonation. Facebook has not supported these measures or requested any organization or chamber of commerce to do so.

In 2016, Senator Terry Link, the author of the Illinois Biometric Information Privacy Act, introduced a measure (HB 6074) clarifying that the original law (1) does not apply to information derived from physical or digital photographs and (2) uses the term "scan" to mean information that is obtained from an in-person process. These clarifying amendments were consistent with industry's longstanding interpretation of the law and Facebook publicly supported them.

Question 9. Would advocating for changes to the Illinois Biometric Identification Privacy Act be consistent with Facebook's commitment to protecting privacy?

Answer. Facebook's advocacy is consistent with our commitment to protecting privacy. As the findings of the Illinois General Assembly confirm, when people raise privacy concerns about facial recognition, they are generally about specific uses of facial recognition. In enacting the Illinois Biometric Information Privacy Act, the General Assembly explained that its concern was "new applications of biometric-facilitated financial transactions, including finger-scan technologies at grocery stores, gas stations, and school cafeterias."

Facebook's use of facial recognition in our products, on the other hand, is very different. Facebook uses facial-recognition technology with users to provide Facebook users—who choose to join Facebook for the purpose of connecting with and sharing information about themselves with others, and affirmatively agree to Facebook's Terms of Service and Data Policy—with products and features that protect their identities and enhance their online experiences while giving them control over the technology. For example, Facebook uses facial-recognition technology to protect users against impersonators by notifying users when someone else has uploaded a photo of them for use as a profile photo and to enable features on the service to people who are visually impaired. Facebook also uses facial-recognition technology to suggest that people who upload photos or videos tag the people who appear in the photos or videos. When someone is tagged in a photo or video, Facebook automatically notifies that person that he or she has been tagged, which in turn enables that person to take action if he or she does not like the content—such as removing

the tag or requesting that the content be removed entirely. Facebook users have always had the ability to change their settings to prevent Facebook from using facial recognition to recognize them.

Given the very different uses of facial-recognition technology that exist, we believe that a one-size-fits-all approach to regulation of facial-recognition technology is not in the public's best interest, and we believe that clarification that the Illinois Biometric Information Privacy Act was not intended to apply to all uses of facial recognition is consistent with Facebook's commitment to protecting privacy. Furthermore, our commitment to support meaningful, thoughtfully drafted privacy legislation means that we can and do oppose measures that create confusion, interfere with legitimate law enforcement action, create unnecessary risk of frivolous litigation, or place undue burdens on people's ability to do business online.

Question 10. Does Facebook oppose legislative efforts to revise and carve exceptions out of the Illinois Biometric Identification Privacy Act?

Answer. See Responses to Questions 8 and 9.

Question 11. Last October, Facebook's general counsel, Colin Stretch, testified before the Senate Judiciary Subcommittee on Crime and Terrorism. I asked him about a letter that 19 leading civil rights organizations—including Muslim Advocates, The Leadership Conference on Civil and Human Rights, the NAACP, the Arab American Institute, Human Rights Campaign, and the Southern Poverty Law Center—sent to Facebook, which explained their "deep concern regarding ads, pages, and hateful content on your platform used to divide our country, and in particular, to promote anti-Muslim, anti-Black, anti-immigrant, and anti-LGBTQ animus."

The organizations referenced a number of examples that had previously been reported by the media, including a Russian Facebook account that "not only promoted anti-immigrant messaging online, but also managed to organize an in-person anti-refugee rally in Twin Falls, Idaho in August 2016." The letter also alleges that "Facebook offered its expertise to a bigoted advocacy group by creating a case study testing different video formats, and advising on how to enhance the reach of the group's anti-refugee campaign in swing states during the final weeks of the 2016 election."

Mr. Stretch agreed that the content was vile and responded that Facebook was "tightening our content guidelines as they apply to ads with respect to violence."

I know that Facebook has met with the groups that have expressed these concerns, but can you elaborate on the specific, substantive steps that Facebook has taken so far, and plans to take in the future, to combat violent hate content on your platform?

Answer. Facebook has engaged Relman, Dane & Colfax, a respected civil rights law firm, to carry out a comprehensive civil rights assessment of Facebook's services and internal operations. Laura Murphy, a national civil liberties and civil rights leader, will help guide this process—getting feedback directly from civil rights groups, like The Leadership Conference on Civil and Human Rights—and help advise Facebook on the best path forward.

On hate speech specifically, our policies prohibit direct attacks on people based on what we call protected characteristics—race, ethnicity, national origin, religious affiliation, sexual orientation, sex, gender, gender identity, and serious disability or disease. We also provide some protections for immigration status. We define attack as violent or dehumanizing speech, statements of inferiority, or calls for exclusion or segregation, and we separate attacks into three tiers of severity.

We recently updated our hate speech policies to remove violent speech directed at groups of people defined in part by protected characteristics. Under the previous hate speech policy, a direct attack targeting women exclusively on the basis of gender, for example, would have been removed from Facebook, but the same content directed at women drivers would have remained on the platform. We have come to see that this distinction is a mistake, and we no longer differentiate between the two forms of attack when it comes to only the most violent hate speech. We continue to explore how we can adopt a more granular approach to hate speech.

In the last nine months, we have also made significant changes to advertising on Facebook, committing to a more robust ad review process and the hiring of 10,000 more people to aid in our safety and security efforts, increasing ads transparency, and tightening restrictions on advertiser content and targeting.

- *Strengthening enforcement.* Before any ad can appear on Facebook or Instagram, it must go through our ad review process. We rely on both automated and manual review, and we're taking aggressive steps to strengthen both. The process includes automated checks of an ad's images, text, targeting, and positioning, in addition to the content on the ad's Facebook and landing pages. Our automated systems also flag content for human review. We are in-

creasing the size of our security and safety teams from 10,000 to 20,000 over the course of this year, and are simultaneously working to hire more people from African American and Hispanic communities. This will help increase the diversity of our workforce and improve our understanding and awareness of ads that are meant to exploit culturally sensitive issues. In addition, we are investing more in machine learning to better understand when to flag and take down ads.

- *Making advertising more transparent.* We believe that when users see an ad, they should know who ran it and what other ads they're running—which is why we show the Page name for any ads that run in a user's News Feed. To provide even greater transparency for people and accountability for advertisers, we're now building new tools that will allow users to see the other ads a Page is running as well—including ads that aren't targeted to them directly. We hope that this will establish a new standard for our industry in ad transparency. We try to catch content that shouldn't be on Facebook before it's even posted—but because this is not always possible, we also take action when people report ads that violate our policies. We hope that more transparency will mean more people can report inappropriate ads.
- *Tightening restrictions on advertiser content.* We hold people on Facebook to our Community Standards, and we hold advertisers to even stricter guidelines. Our ads policies already prohibit shocking content, direct threats and the promotion of the sale or use of weapons. Going forward, we are expanding these policies to prevent ads that use even more subtle expressions of violence.
- *Changes to advertiser targeting.* Being able to direct ads at a particular audience is particularly valuable for businesses and for people, but it's important that this be done in a safe and civil way. That's why we've been closely reviewing the targeting options we offer. Even though targeting is an important tool to reach people, we have heard concerns about potential abuse, particularly about the feature that lets advertisers exclude people from their ads. Advertisers want to show ads to people most likely to be interested in their offerings, and exclusion targeting helps avoid showing ads to people who likely aren't interested. For example, if a local basketball team is trying to attract new fans, they can exclude people who are already interested in the team. In response to the feedback we've received, we've removed thousands of categories from exclusion targeting. We focused mainly on topics that relate to potentially sensitive personal attributes, such as race, ethnicity, sexual orientation, and religion. Our review is continuous; the process will be ongoing and we'll continue soliciting feedback. We take our responsibility to keep advertising safe and civil seriously, and we will keep exploring more ways to make targeting work for people and businesses.

Question 12. We have also seen the impact of hate content on the international stage. In Myanmar, United Nations investigators have found that Facebook has played a "determining role" in violence against the Muslim Rohingya population.

Specifically, the chairman of the U.N. Independent International Fact-Finding Mission on Myanmar told reporters that social media "has . . . substantively contributed to the level of acrimony and dissension and conflict, if you will, within the public. Hate speech is certainly of course a part of that. As far as the Myanmar situation is concerned, social media is Facebook, and Facebook is social media." Another investigator said that Facebook was used by ultra-nationalists who were "inciting a lot of violence and a lot of hatred against the Rohingya or other ethnic minorities."

In a recent interview with *Vox,* you suggested that Facebook's systems had detected inflammatory, widely-shared chain letters about imminent attacks, and that Facebook stopped those messages. In reality, a group of Myanmar civil society organizations had flagged this content, and the messages were shared thousands of times for three days before Facebook took steps to prevent the spread of the messages. After your interview, these organizations sent you a letter noting "this case exemplifies the very opposite of effective moderation: it reveals an over-reliance on third parties, a lack of a proper mechanism for emergency escalation, a reticence to engage local stakeholders around systemic solutions and a lack of transparency." I understand that you have personally responded to these organizations and that they have sent you a follow-up letter asking for additional information on how Facebook is addressing these issues.

The situation in Myanmar is not unique. Violent anti-Muslim content is also widely shared in Sri Lanka and recently led the Sri Lankan government to temporarily ban access to Facebook. A recent *Buzzfeed* report stated:

> Government officials, researchers, and local NGOs say they have pleaded with Facebook representatives from as far back as 2013 to better enforce the company's own rules against using the platform to call for violence or to target people for their ethnicity or religious affiliation. They repeatedly raised the issue with Facebook representatives in private meetings, by sharing in-depth research, and in public forums. The company, they say, did next to nothing in response.
>
> Ethnic tensions run deep in Sri Lanka, particularly between the majority Sinhala Buddhists and minority groups, and the country has seen a troubling rise in anti-Muslim hate groups and violence since the end of its decades-long civil war in 2009. Many of those hate groups spread their messages on Facebook. The problem came to a head in March when Buddhist mobs in central Sri Lanka burned down dozens of Muslim shops, homes, and places of worship.

a. What is your response to these reports?

b. What steps is Facebook taking to address anti-Muslim hate content in countries like Sri Lanka and Myanmar?

Answer. We've been too slow to deal with the hate and violence in places like Myanmar and Sri Lanka. The challenges we face in a country that has fast come online are very different than those in other parts of the world, and we are investing in people, technology, and programs to help address them as effectively as possible.

We are increasing the number of Burmese and Sinhalese-language content reviewers as we continue to grow and invest in Myanmar and Sri Lanka. Our goal is always to have the right number of people with the right native language capabilities to ensure incoming reports are reviewed quickly and effectively. That said, there is more to tackling this problem than reported content. A lot of abuse may go unreported, which is why we are supplementing our hiring with investments in technology and programs.

We are building new tools so that we can more quickly and effectively detect abusive, hateful, or false content. We have, for example, designated several hate figures and organizations for repeatedly violating our hate speech policies, which has led to the removal of accounts and content that support, praise, or represent these individuals or organizations. We are also investing in artificial intelligence that will help us improve our understanding of dangerous content.

We are further strengthening our civil society partner network so that we have a better understanding of local context and challenges. We are focusing on digital literacy education with local partners in Myanmar and Sri Lanka. For example, we launched a local language version of our Community Standards to educate new users on how to use Facebook responsibly in 2015 and we have been promoting these actively in Myanmar, reaching over 8 million people through promotional posts on our platform alone. We've also rolled out several education programs and workshops with local partners to update them on our policies and tools so that they can use this information in outreach to communities around the country. One example of our education initiatives is our work with the team that developed the Panzagar initiative (*https://www.facebook.com/supportflowerspeech*) to develop the Panzagar counterspeech Facebook stickers to empower people in Myanmar to share positive messages online. We also recently released locally illustrated false news tips, which were promoted on Facebook and in consumer print publications. We have a dedicated Safety Page for Myanmar (*https://www.facebook.com/safety/resources/myanmar*) and have delivered hard copies of our local language Community Standards and safety and security tips to civil society groups in Myanmar who have distributed them around the country for trainings. Similarly, in Sri Lanka, we ran a promotion in English, Sinhalese, and Tamil at the top of News Feeds in April 2017 to educate people on our Community Standards, in particular hate speech. The content has been viewed almost 100M times by almost 4M people.

Question 13. When I chaired the Senate Judiciary Subcommittee on Human Rights and the Law, I held a series of hearings on Internet freedom. I invited Facebook to testify at our 2010 hearing. Unlike Google, Yahoo, and Microsoft, Facebook declined.

Beginning in 2009, I urged you and other technology companies to join the Global Network Initiative, a voluntary code of conduct that requires participating companies to take reasonable measures to protect human rights. Again, unlike Google, Yahoo, and Microsoft, you declined.

I reached out to you again in 2011 about serious concerns that repressive governments were using Facebook to monitor and suppress democracy activists.

I was glad when Facebook finally joined other major technology companies and became a member of the Global Network Initiative in 2013. But it's also clear that

Facebook has lagged behind other technology leaders in this area and that you continue to face serious ongoing human rights challenges.

For example, human rights activists in Vietnam have expressed concerns that Facebook is working with the Vietnamese government to suppress dissent. A number of Vietnamese human rights activists and independent media groups sent a letter to you yesterday that noted "your company's aggressive practices . . . could silence human rights activists and citizen journalists in Vietnam."

The letter went on to say the following: "We appreciate Facebook's efforts in addressing safety and misinformation concerns online in Vietnam and around the world. Yet it would appear that after this high profile agreement to coordinate with a government that is known for suppressing expression online and jailing activists, the problem of account suspension and content takedown has only grown more acute."

a. Can you comment on Facebook's commitment to human rights?

b. What is your response to this letter?

c. How is Facebook addressing free expression and user privacy concerns in countries with repressive regimes?

Answer. Facebook is committed to respecting human rights. Since 2013, Facebook has been a member of the Global Network Initiative (GNI), a multi-stakeholder digital rights initiative. As part of our membership, Facebook has committed to the freedom of expression and privacy standards set out in the GNI Principles—which are in turn based on the Universal Declaration of Human Rights and the United Nations Guiding Principles on Business and Human Rights—and we are independently assessed on our compliance with these standards on a biennial basis. In keeping with these commitments, rigorous human rights due diligence and careful consideration of free expression and privacy implications would constitute important components of any decision on entering China.

As a GNI member, Facebook is committed to privacy and free expression principles and implementation guidelines regarding government requests. The GNI standards have been shaped by international human rights laws and norms and developed through a robust multi-stakeholder and consultative process. The GNI principles and guidelines inform Facebook's approach to evaluating government requests for user data in all the markets where we operate.

Regarding the letter from Vietnamese human rights activists and citizen journalists specifically, we are committed to protecting the rights of people using Facebook in Vietnam, and to providing a place where people can express themselves freely and safely.

- Our Community Standards (*https://www.facebook.com/communitystandards*), which outline what is and isn't allowed on Facebook, seek to encourage expression and create a safe community on the platform. We will remove content that violates these standards when we're made aware of it.
- There are also times when we may have to remove or restrict access to content because it violates a law in a particular country, even though it doesn't violate our Community Standards. We have a well-established process for this, which is no different in Vietnam to the rest of the world. Every request we receive is checked for legal sufficiency. We require officials to provide a detailed description of the legal and factual basis for their request, and we push back when we find legal deficiencies or overly broad or vague requests. We report the number of pieces of content we restrict for contravening local law in our Transparency Report.
- We did not take any action on the accounts of the signatories of the letter at the request of the Vietnamese government, nor did we see mass reporting on their accounts.
- We continue to work with partners in industry and civil society to voice concerns about efforts to restrict expression and limit the voice that people have online.

Question 14. Open Secrets recently reported that multimillionaire donor Robert Mercer was behind a secretive dark money group called Secure America Now. According to Open Secrets, this organization "worked hand in hand with Facebook and Google to target their message at voters in swing states who were most likely to be receptive to them."

Specifically, Secure America Now created mock travel ads that invited visitors to the "Islamic State of France," the "Islamic State of Germany," and the "Islamic States of America." Each ad began with an image of missiles shooting through the sky. The "French" ad included clips of blindfolded men with guns held to their head and children training with weapons. The "German" ad discussed "sell[ing] your

daughter or sister to be married" with the image of a woman wearing a burka. The "American" ad had an image of Ground Zero in New York City as a place where citizens "celebrate Islamic victories."

The ads were clearly designed to stoke anti-Muslim sentiment in the days leading up to the 2016 election.

a. Under your new policies, how will ads like this be handled in the future?

b. Will Facebook continue to work with groups like Secure America Now to create targeted, bigoted content?

Answer. We did not work directly with Secure America Now; we worked through a third-party advertising agency. We did not create any content for Secure America Now. As is customary across managed advertising agencies, we provided a general best practices training to the agency staff, and we provided the measurement tools to determine the efficacy of the ads and differences between formats.

We require everyone on Facebook to comply with our Community Standards, which outline what is and isn't allowed on Facebook.

Explicit in our Community Standards is our prohibition on hate speech. We are opposed to hateful content in all its forms, and are committed to removing it from our platform any time we become aware of it. We're also committed to getting better at addressing these issues, including improving specific policies, our review process, and community reporting.

We have Community Standards that prohibit hate speech, bullying, intimidation and other kinds of harmful behavior. We hold advertisers to even stricter advertising policies to protect people from things like discriminatory ads—and we have recently tightened our ad policies even further to prohibit additional shocking and sensational content.

Question 15. As you noted in your testimony, before the 2017 French election Facebook found and took down 30,000 fake accounts. Will you commit to inform Congress and the public on a real-time basis how many fake accounts Facebook takes down in the lead-up to the 2018 U.S. midterm elections?

Answer. We recently released enforcement statistics in our Community Standards Enforcement Report, including how many Facebook accounts we took action on because we determined they were fake. We will refine our approach over time, and we also hope to release additional metrics in future reports.

Question 16. What percentage of current Facebook accounts do you understand or estimate to be fake?

Answer. We estimate that fake accounts represented approximately 3 percent to 4 percent of monthly active users (MAU) on Facebook during Q1 2018 and Q4 2017. We share this number in the Facebook quarterly financial results. This estimate may vary each quarter based on spikes or dips in automated fake account creation.

Question 17. I assume there is an advertising revenue loss when Facebook deletes an account that is active but that is a fake or imposter account created to sow disinformation. But it is important for the public and Congress to know how many of these accounts there are and whether they are being removed.

a. Will Facebook be transparent with Congress and the public about how many active fake accounts Facebook is deleting?

b. How will Facebook enable Congress to track your progress in addressing and removing fake accounts?

Answer. We publish information and metrics about fake accounts at *https://transparency.facebook.com/community-standards-enforcement#fake-accounts* and in our SEC filings. We estimate that fake accounts represented approximately 3 percent to 4 percent of monthly active users (MAU) on Facebook during Q1 2018 and Q4 2017. We share this number in the Facebook quarterly financial results. This estimate may vary each quarter based on spikes or dips in automated fake account creation.

Question 18. You say in your testimony that Facebook now has about 15,000 people working on security and content review. How many of those people are dedicated to identifying and removing fake accounts?

Answer. Estimating a number is difficult because stopping this type of abuse is a focus for many teams, some more directly and some in more of a supportive role. For example, we are expanding our threat intelligence team, and more broadly, we are working now to ensure that we will more than double the number of people working on safety and security at Facebook, from 10,000 to 20,000, by the end of 2018. We expect to have at least 250 people specifically dedicated to safeguarding election integrity on our platforms, and that number does not include the thousands of people who will contribute to this effort in some capacity. Many of the people we are adding to these efforts will join our ad review team, and we also expect to add

at least 3,000 people to Community Operations, which reviews content that our users and automated tools flag as inappropriate, dangerous, abusive, or otherwise violating our policies.

Question 19. You stated during your testimony that Facebook has built A.I. tools for identifying terror and extremist-related content and that, for example, 99 percent of the ISIS and al-Qaeda content that Facebook takes down is flagged first via A.I.

a. How much content did Facebook take down that was linked to ISIS and al-Qaeda and what was the basis of your 99 percent statistic? Please quantify this in terms of accounts closed per year or some other quantifiable metric.

b. How much extremist content does Facebook take down that is not first identified by A.I.? Please quantify this in terms of accounts closed per year.

c. How much extremist content would you estimate is not removed by Facebook because it is not flagged by A.I. or by users?

d. We are facing a rising threat from white supremacist and other domestic extremist groups. An unclassified May 2017 FBI–DHS joint intelligence bulletin found that "white supremacist extremism poses [a] persistent threat of lethal violence," and that white supremacists "were responsible for 49 homicides in 26 attacks from 2000 to 2016 . . . more than any other domestic extremist movement." And *Politico* reported in August 2017 that "suspects accused of extreme right-wing violence have accounted for far more attacks in the U.S. than those linked to foreign Islamic groups like al Qaeda and ISIS, according to multiple independent studies." What specific steps is Facebook taking to address extremist content from white supremacists and other domestic terrorist threats?

Answer. While these metrics are in development, in Q1 2018, we took action on 1.9 million pieces of terrorist propaganda content related to ISIS, al-Qaeda, and their affiliates, up from 1.1 million in Q4 2017. This increase is due to improvements in our ability to find violating content using photo detection technology, which detects both old content and newly posted content.

While these metrics are in development, in Q1 2018, we found and flagged 99.5 percent of the terrorist propaganda content related to ISIS, al-Qaeda, and their affiliates we subsequently took action on, before users reported it. We acted on the other 0.5 percent because users reported it to us first. The amount of content we flagged increased from around 97 percent in Q4 2017 because we improved our photo detection technology and processes to find and flag more content before users reported it.

Terrorists, terrorist content, and hate speech in all forms—including white supremacy and domestic terrorist content—have no place on Facebook. We prohibit content that incites violence, and we remove terrorists and posts that support terrorism whenever we become aware of them. We are using a variety of tools in this fight.

Our policies against terrorist organizations and hate organizations fall within the broader category of dangerous organizations and individuals. We do not want Facebook to be a platform for hatred or violence, so our policies apply to all groups that have engaged in premeditated acts of violence or attacks on the basis of race, religious affiliation, nationality, ethnicity, gender, sex, sexual orientation, and serious disease or disability.

We define terrorism as "Any non-governmental organization that engages in premeditated acts of violence against persons or property to intimidate a civilian population, government, or international organization in order to achieve a political, religious, or ideological aim." Our definition is agnostic to the ideology or political goals of a group, which means it includes everything from religious extremists and violent separatists to white supremacists and militant environmental groups. It's about whether they use violence to pursue those goals.

We are equally committed to identifying and rooting out domestic hate organizations. We define hate organizations as "Any association of three or more people that is organized under a name, sign, or symbol and that has an ideology, statements, or physical actions that attack individuals based on characteristics, including race, religious affiliation, nationality, ethnicity, gender, sex, sexual orientation, and serious disease or disability." In evaluating groups and individuals for designation as hateful, we have an extensive process that takes into account a number of different signals, and regularly engage with academics and organizations to refine this process.

Question 20. If Facebook's users have their personal information misused without their knowledge and consent and then seek redress in the court system, it is possible that the companies that misused their information will try to force Facebook's users into mandatory arbitration proceedings. These arbitration proceedings are

typically kept secret and rules are titled in favor of the repeat corporate player and against the victims.

a. Do you think it is fair for Facebook users to be forced into mandatory arbitration when they are trying to seek redress for companies' misuse of their personal information?

b. Does Facebook prohibit apps that use the Facebook platform from using mandatory arbitration clauses on Facebook users? If not, will you commit to doing so going forward?

Answer. Our Terms of Service, available at *https://www.facebook.com/terms.php*, addresses dispute resolution for users and our Platform Policy, available at *https://developers.facebook.com/policy*, lists the requirements for developers. Facebook's Terms do not contain an arbitration clause and, in fact, we recently updated our Terms to make it easier for users outside of the United States to access court systems in their home countries.

Question 21. In December, the Federal Communications Commission (FCC) voted to dismantle net neutrality rules, paving the way for Internet providers to block, throttle, or manipulate consumer access to the Internet. This action threatens the right of every consumer to access a free and open internet.

In the past, Facebook has expressed support for net neutrality protections.

a. As one of the most visited websites in the world, how important is net neutrality to Facebook's mission?

b. If left unchanged, what impact will the FCC's decision to undo net neutrality protections have on Facebook's millions of users?

Answer. Keeping the Internet open for everyone is crucial. Not only does it promote innovation, but it lets people access information that can change their lives and gives voice to those who might not otherwise be heard. For these reasons, Facebook supports net neutrality and is open to working members of Congress and anyone else on a solution that will preserve strong net neutrality protections.

RESPONSE TO WRITTEN QUESTIONS SUBMITTED BY HON. SHELDON WHITEHOUSE TO MARK ZUCKERBERG

Question 1. Your written testimony referenced a number of policies Facebook has planned or implemented to prevent foreign nationals from using the platform to interfere in political and electoral processes.

a. How will you ensure that the companies advertising on Facebook are who they purport and claim to be, rather than fronts for otherwise prohibited users?

b. Do shell corporations impede your company's progress in preventing abuse of your platform by foreign agents? If so, how?

c. Would incorporation transparency laws requiring the disclosure of beneficial ownership information at the time of incorporation enhance your ability to overcome those impediments?

Answer. We announced that only authorized advertisers will be able to run electoral ads on Facebook or Instagram. And we're also extending that requirement to anyone that wants to show "issue ads"—like political topics that are being debated across the country. We are working with third parties to develop a list of key issues, which we will refine over time. To get authorized by Facebook, advertisers will need to confirm their identity and location. Advertisers will be prohibited from running political ads—electoral or issue-based—until they are authorized.

Further, we have processes designed to identify inauthentic and suspicious activity and we also maintain a sanctions compliance program to screen advertisers and paid app developers. Facebook's denied party screening protocol involves checking paid app developers and advertisers against applicable denied party listings. Those screened remain in an on-going monitoring portfolio and are screened against changes to applicable denied party listings. Moreover, our payments subsidiaries file Suspicious Activity Reports on developers of certain apps as appropriate.

However, like other offline and online companies, Facebook has limited insight into the use of shell corporations or other sophisticated structures that may disguise the true buyer. In addition, the general challenge of attributing online activities to specific governments or organizations is widely recognized in the intelligence and law enforcement communities.

It is possible that such laws could help companies gain insight into the use of shell corporations or other sophisticated structures that may disguise the true buyer.

Question 2. With respect to the exchange below, is there anything you would like to add to your statements about the process whereby Facebook required Cambridge

Analytica to certify that it had deleted all improperly acquired data? Can you confirm that Facebook entered into a legally binding contract with Cambridge Analytica surrounding the deletion of unlawfully obtained user data? Would you be willing to share a copy of the contract in question with the Senate Committees before which you appeared, if so?

WHITEHOUSE: And with respect to Cambridge Analytica, your testimony is that first you required them to formally certify that they had deleted all improperly acquired data. Where did that formal certification take place? That sounds kind of like a quasi-official thing, to formally certify. What did that entail?

ZUCKERBERG: Senator, first they sent us an e-mail notice from their chief data officer telling us that they didn't have any of the data any more, that they deleted it and weren't using it. And then later we followed up with, I believe, a full legal contract where they certified that they had deleted the data.

WHITEHOUSE: In a legal contract?

ZUCKERBERG: Yes, I believe so.

On December 11, 2015, *The Guardian* published an article reporting that Kogan and his company, GSR, may have passed information the app had obtained from Facebook users to SCL Elections Ltd. (SCL)/Cambridge Analytica. If this occurred, Kogan and his company violated Facebook's Platform Policies, which explicitly prohibited selling user data accessed from Facebook and from sharing any user data accessed from Facebook with any ad network, data broker, or other advertising or monetization related service.

For this reason, Facebook immediately banned the app from our platform and investigated what happened and what further action we should take to enforce our Platform Policies. Facebook also contacted Kogan/GSR and demanded that they explain what data they collected, how they used it, and to whom they disclosed it. Facebook further insisted that Kogan and GSR, as well as other persons or entities to whom they had disclosed any such data, account for and irretrievably delete all such data and information.

Facebook also contacted Cambridge Analytica to investigate the allegations reflected in the reporting. On January 18, 2016, Cambridge Analytica provided written confirmation to Facebook that it had deleted the data received from Kogan and that its server did not have any backups of that data. On June 11, 2016, Kogan executed and provided to Facebook signed certifications of deletion on behalf of himself and GSR. The certifications also purported to identify all of the individuals and entities that had received data from GSR (in addition to Kogan and his lab), listing the following: SCL, Eunoia Technologies (a company founded by Christopher Wylie), and a researcher at the Toronto Laboratory for Social Neuroscience at the University of Toronto. On July 7, 2016, a representative of the University of Toronto certified that it deleted any user data or user-derived data. On August 16, 2016, Eunoia (executed by Eunoia Founder Christopher Wylie) certified that it deleted any user and user-derived data. On September 6, 2016, counsel for SCL informed counsel for Facebook that SCL had permanently deleted all Facebook data and derivative data received from GSR and that this data had not been transferred or sold to any other entity. On April 3, 2017. Alexander Nix, on behalf of SCL, certified to Facebook, that it deleted the information that it received from GSR or Kogan.

Because all of these concerns relate to activity that took place off of Facebook and its systems, we have no way to confirm whether Cambridge Analytica may have Facebook data without conducting a forensic audit of its systems. Cambridge Analytica has agreed to submit to a forensic audit, but we have not commenced that yet due to a request from the UK Information Commissioner's Office, which is simultaneously investigating Cambridge Analytica (which is based in the UK). And even with an audit, it may not be possible to determine conclusively what data was shared with Cambridge Analytica or whether it retained data after the date it certified that data had been deleted.

The existing evidence that we are able to access supports the conclusion that Kogan only provided SCL with data on Facebook users from the United States. While the accounts of Kogan and SCL conflict in some minor respects not relevant to this question, both have consistently maintained that Kogan never provided SCL with any data for Facebook users outside the United States. These consistent statements are supported by a publicly released contract between Kogan's company and SCL.

Question 3. Until 2014, Facebook allowed "friend permissiosn," which meant that if one of your Facebook friends connected an authorized app to his Facebook account, the app could access not only that person's personal information, but also your personal information—and all of his other friends' personal information—re-

gardless of his friends' privacy settings. Facebook rightly changed that permission in 2014.

a. Do you have an estimate as to how many third party entities were authorized to collect friends' data while "friend permission" was in effect?

b. Do you know what happened to that data and whether it was shared further?

Answer. We are in the process of investigating every app that had access to a large amount of information before we changed our Platform in 2014. The investigation process is in full swing, and it has two phases. First, a comprehensive review to identify every app that had access to this amount of Facebook data and to focus on apps that present reason for deeper investigation. And second, where we have concerns, we will conduct interviews, make requests for information (RFI)—which ask a series of detailed questions about the app and the data it has access to—and perform audits using expert firms that may include on-site inspections. We have large teams of internal and external experts working hard to investigate these apps as quickly as possible. To date thousands of apps have been investigated and around 200 apps have been suspended—pending a thorough investigation into whether they did in fact misuse any data. Where we find evidence that these or other apps did misuse data, we will ban them and let people know.

These apps relate to a handful of developers: Kogan, AIQ, Cube You, the Cambridge Psychometrics Center, and myPersonality, with many of the suspended apps being affiliated with the same entity. Many of theses suspensions include apps that appear to be "test" apps that were never released to the public, and therefore would not have acquired significant user data, although our investigation into these apps is ongoing.

Additionally, we have suspended an additional 14 apps, which were installed by around one thousand people. They were all created after 2014, after we made changes to more tightly restrict our platform APIs to prevent abuse. However, these apps appear to be linked to AIQ, which was affiliated with Cambridge Analytica. So, we have suspended them while we investigate further. Any app that refuses to take part in or fails our audit will be banned.

We will commit to briefing your staff on future developments.

c. How does Facebook audit third party applications to ensure that they are who they say they are?

Answer. In general, on an ongoing basis, we proactively review all apps seeking access to more than basic information (and have rejected more than half of apps seeking such extended permissions). We also do a variety of manual and automated checks to ensure compliance with our policies and a positive experience for people. These include steps such as random checks of existing apps along with the regular and proactive monitoring of apps. We also respond to external or internal reports and investigate for potential app violations. When we find evidence of or receive allegations of violations, we investigate and, where appropriate, employ a number of measures, including restricting applications from our platform, preventing developers from building on our platform in the future, and taking legal action where appropriate.

d. Do users have a way of tracking what data about them was shared with third parties, including when this data is shared by their friends? Should they?

Answer. With respect to our investigation into apps that had access to large amounts of information, if we find evidence that these or other apps did misuse data, we will ban them and notify people whose data was shared with these apps.

Question 4. Aleksander Kogan purported to be a researcher when he came to Facebook with the app Thisisyourdigitallife. He then funneled the information he collected about Facebook's users to Cambridge Analytica, which planned to use that information to influence Facebook users' political opinions. How was Dr. Kogan vetted? What policies and procedures does Facebook follow to ensure that researchers are who they say they are and that their research is legitimate?

Answer. Facebook was put in touch with Kogan (a researcher at the University of Cambridge) in late 2012, about a possible collaboration on research relating to the potential relationship between Facebook friendship ties and economic trade volumes between countries. Kogan collaborated with current and former Facebook employees on approximately ten academic papers. As part of these collaborations, Kogan could only access fully anonymized, aggregated data from Facebook. Facebook frequently partners with leading academic researchers to address topics pertaining to wellbeing, innovation, and other topics of public importance, following strict protocols to ensure personal information is safeguarded.

Question 5. The General Data Protection Regulation (GDPR) goes into effect in Europe in May. It will require that users be afforded meaningful opportunities for informed consent and the ability to opt-out of direct marketing. It will also require

data portability and give users the right to access their personal data. Finally, it will mandate privacy by design and require that users be informed within 72 hours of a data breach. What is Facebook doing in Europe to get ready to comply with GDPR?

Answer. The GDPR requires companies to obtain explicit consent to process certain kinds of data ("special categories of data" like biometric data). We are seeking explicit consent from people in Europe to three specific uses of data: facial recognition data (which previously was not enabled in Europe), special categories of data, and use of data we collect off Facebook Company Products to target ads. We recently began providing direct notice of these controls and our updated terms to people around the world (including in the U.S.), allowing people to choose whether or not to enable or disable these settings or to agree to our updated terms. Outside of Europe we are not requiring people to complete those flows if they repeatedly indicate that they do not want to go through the experience. At the same time, the events of recent months have underscored how important it is to make sure people know how their information is used and what their choices are. So, we decided to communicate prominently on Facebook—through a full-screen message and a reminder to review at a later date. People can choose to dismiss or ignore these messages and continue using Facebook.

We are also upgrading our tools for access, rectification, erasure, data portability, and others to people in the U.S. and rest of world that we provide in Europe, and many of those tools (like our Download Your Information tool, Ads Preferences tool, and Activity Log) have been available globally for many years.

Many of the requirements under GDPR previously applied to Facebook Ireland under the Data Protection Directive, and we have therefore been following these principles for many years. The GDPR is founded on core principles of transparency and control, which are also central values we employ in designing our products.

Question 6. You've made headlines recently by saying that Facebook will not apply all of GDPR in the United States. Which GDPR requirements is Facebook choosing not to apply in the U.S.? Why? What parts of GDPR do you think the U.S. should import?

Answer. The controls and settings that Facebook is enabling as part of GDPR are available to people around the world, including settings for controlling our use of face recognition on Facebook and for controlling our ability to use data we collect off Facebook Company Products to target ads. We recently began providing direct notice of these controls and our updated terms to people around the world (including in the U.S.), allowing people to choose whether or not to enable or disable these settings or to consent to our updated terms. We provide the same tools for access, rectification, erasure, data portability and others to people in the U.S. and rest of world that we provide in Europe, and many of those tools (like our Download Your Information tool, ad preferences tool, and Activity Log) have been available globally for many years.

Question 7. Facebook has announced that it will begin placing ads into a searchable database, which will include details about how much the ads cost and what kinds of people the advertisers were targeting. Ads will stay in the database for four years. Will the database include information on the audience that advertisers were *trying* to target or just the demographic information about which users were ultimately reached?

Answer. The database will include demographic information (*e.g.,* age, general location, gender) about the audience that the ads reached.

Question 8. As Chair of the Cybersecurity Task Force and a Co-Chair of the International Creativity and Theft-Prevention Caucus, I have focused time and attention on the issue of platform security and responsibility—including as it relates to intellectual property theft. What steps is Facebook taking to ensure that it provides a safe and secure platform in this respect? Will you devote the resources necessary to ensure that your platform and its features/tools, including Facebook Live, are used in a responsible and legal fashion?

Answer. We take intellectual property rights seriously at Facebook and work closely with the motion picture industries and other rights holders worldwide to help them protect their copyrights and other IP. Our measures target potential piracy across our products, including Facebook Live, and continue to be enhanced and expanded. These include a global notice-and-takedown program, a comprehensive repeat infringer policy, integration with the content recognition service Audible Magic, and our proprietary video- and audio-matching technology called Rights Manager. More information about these measures can be found in our Intellectual Property Help Center, Transparency Report, and Rights Manager website.

Question 9. Your Q3 earnings disclosure in 2017 indicated that over 270 million Facebook accounts are fake or duplicate accounts. Fake and imposter accounts have been identified as central to the disinformation campaigns threatening democracies, and you have responded by banning tens of thousands of these accounts to protect elections in France, Germany, and Alabama. Do you intend to enforce your user policy and track and delete as many fake and imposter accounts on your site as possible and, if so, on what timeline? Are there circumstances under which Facebook would track, but opt not to delete, inauthentic accounts that may be involved in disinformation campaigns? What would such circumstances be?

Answer. We are committed to finding and removing fake accounts. We continue to make improvements to our efforts to more effectively detect and deactivate fake accounts to help reduce the spread of spam, false news, and misinformation. We continually update our technical systems to identify, checkpoint, and remove inauthentic accounts, and we block millions of attempts to register fake accounts every day. These systems examine thousands of detailed account attributes and prioritize signals that are more difficult for bad actors to disguise, such as their connections to others on our platform. As with all security threats, we have been incorporating new insights into our models for detecting fake accounts, including information specific to election issues.

We do not share detailed descriptions of how our tools work in order to avoid providing a road map to bad actors who are trying to avoid detection. When we suspect that an account is inauthentic, we typically enroll the account in a checkpoint that requires the account holder to provide additional information or verification. We view disabling an account as a severe sanction, and we want to ensure that we are highly confident that the account violates our policies before we take permanent action. When we have confirmed that an account violates our policies, we remove the account.

Question 10. (a) How does Facebook define fake news?

(b) How does the company distinguish real news stories from fake ones, if at all?

(c) What mechanisms, if any, does Facebook use to prevent news stories identified as fake from appearing on users' news feeds?

(d) Does Facebook keep track of users who exhibit a pattern of sharing fake news stories? Does it suspend users who exhibit such a pattern? If not, would Facebook consider implementing a policy that disciplines users who spread fake news? What else could Facebook do to stop the spread of fake news?

Answer. At Facebook, we define false news as "[n]ews articles that purport to be factual, but which contain intentional misstatements of fact with the intention to arouse passions, attract viewership, or deceive."

We believe that tech companies, media companies, newsrooms, and educators all need to work together to address this societal problem. We are engaged with partners across these industries to help create a more informed community.

We are working to build a more informed community by promoting trustworthy, informative, and local news and by focusing on four different strategies to address misinformation:

- *Strengthening enforcement of our authenticity policies.* We are investing heavily in new technology and hiring thousands more people to tackle the problem of inauthenticity on the platform. Fake accounts are often associated with false news, so this is an area that will have a huge impact on curbing the spread of inaccurate information.
- *Finding industry solutions.* All of us—from tech companies and media companies to newsrooms and classrooms—must work together to find industry solutions to strengthen the online news ecosystem and our own digital literacy. That's why we're collaborating with others who operate in this space. Last January, we announced The Facebook Journalism Project, an initiative that seeks to establish stronger ties between Facebook and the news industry. The project is focused on developing news products, providing training and tools for journalists, and working with publishers and educators on how we can equip people with the knowledge they need to be informed readers in the digital age. Since launching the Journalism Project, we've met with more than 2,600 publishers around the world to understand how they use our products and how we can make improvements to better support their needs.
- *Disrupting economic incentives*. When it comes to fighting false news, we've found that a lot of it is financially motivated. So, one of the most effective approaches is removing the economic incentives for those who traffic in inaccurate information. We've done things like block ads from pages that repeatedly share

false news and significantly limit the distribution of web pages that deliver low quality web experiences.

- *Building new products*. We believe it's important to amplify the good effects of social media and mitigate the bad—to contribute to the diversity of ideas, information, and view points, while strengthening our common understanding. Among the products we've launched is:
  - We believe giving people more context can help them decide what to trust and what to share. The third-party fact-checking program we have developed uses reports from our community, along with other signals, to send stories to accredited third-party fact checking organizations. If the fact checking organizations identify a story as fake, we will suggest related articles in News Feed to show people different points of view, including information from fact checkers. Stories that have been disputed may also appear lower in News Feed. Our own data analytics show that a false rating from one of our fact checking partners reduces future impressions on Facebook by 80 percent.
  - We're also testing Article Context as a way of giving people more information about the material they're reading on Facebook. Since we launched this test, some of the articles people see in News Feed will feature an "i" icon that allows them to access more information at the tap of a button. The information we surface is pulled from across the internet, and includes things like the publisher's Wikipedia entry, trending articles or related articles about the topic, and information about how the article is being shared on Facebook. In some cases, if that information is unavailable, we will let people know since that can also be helpful context.

Question 11. It is my understanding that Facebook currently restricts notifications related to fake news to users who seek to share the content in question. In other words, before sharing a story flagged as fake on the site, a user will receive a warning that the story's accuracy has been "disputed." Does Facebook intend to expand the existing policy and begin notifying individual users each time they view (not just share) fake content? If not, why not?

Answer. As we announced in December 2017, we will no longer use Disputed Flags to identify false news. Instead, we will use Related Articles to help give people more context about the story. Academic research on correcting misinformation has shown that putting a strong image, like a red flag, next to an article may actually entrench deeply held beliefs—the opposite effect to what we intended. Related Articles, by contrast, are simply designed to give more context, which our research has shown is a more effective way to help people get to the facts. Indeed, we have found that when we show Related Articles next to a false news story, it leads to fewer shares than when the Disputed Flag is shown.

We are giving people more context about the information they see on Facebook with Article Context. Since we launched this test, some of the articles you see in News Feed will feature an "i" icon that allows you to access more information at the tap of a button. The information we surface is pulled from across the internet, and includes things like the publisher's Wikipedia entry, trending articles or related articles about the topic, and information about how the article is being shared on Facebook. In some cases, if that information is unavailable, we will let people know since that can also be helpful context.

We continue to look for opportunities to improve this experience and help give people more context so that they can decide what to read, trust, and share on Facebook.

RESPONSE TO WRITTEN QUESTIONS SUBMITTED BY HON. AMY KLOBUCHAR TO MARK ZUCKERBERG

Question 1. In the hearing, I asked if Facebook had determined whether the up to 87 million Facebook users whose data was shared with Cambridge Analytica were concentrated in certain states. You said that you could follow up with that information.

- Can you provide a state-by-state breakdown of the Facebook users whose data was improperly obtained by Cambridge Analytica?

Answer. See the state breakdown here: *https://fbnewsroomus.files.wordpress.com/2018/05/state-by-state-breakdown.pdf*.

Question 2. As you know, I also asked whether any of the roughly 126 million people who may have been shown content from a Facebook page associated with the

Internet Research Agency were the same Facebook users whose data was shared with Cambridge Analytica. You said that Facebook was investigating that question and that you believe it is "entirely possible that there will be a connection there."

- Please provide an answer as to whether there was any overlap between the Facebook users who were shown content from a Facebook page associated with the Internet Research Agency and those whose data was shared with Cambridge Analytica.

Answer. The targeting for the IRA ads that we have identified and provided to the Senate Committee on the Judiciary and the Senate Select Committee on Intelligence was relatively rudimentary, targeting very broad locations and interests, and for example, only used custom audiences in a very small percentage of its overall targeting and did not use Contact List Custom Audiences. In addition, all of the custom audiences used by the IRA were created based on user engagement with certain IRA Pages. By contrast, Cambridge Analytica used hundreds of Contact List Custom Audiences during the 2016 election cycle created from contact lists that Cambridge Analytica uploaded to our system, and Cambridge Analytica used those and other custom audiences in the majority of its ads targeting in combination with demographic targeting tools.

Question 3. When I asked if you would support a rule that would require Facebook to notify users of a breach of their information within 72 hours, you responded that such a rule makes sense to you and that your team would follow up with my staff to discuss the details of such a proposal.

- I am working to introduce bipartisan legislation requiring that online platforms notify users of a breach of their information within 72 hours. Will Facebook support this requirement?
- What process would Facebook implement to notify users of a breach of their information within 72 hours?

Answer. Facebook is generally open to the idea of breach notification requirements, particularly legislation that would centralize reporting and ensure a consistent approach across the United States. For example, in Europe, the GDPR requires notification to a lead supervisory authority, rather than individual member states, in cases of a data breach. In the United States, however, there is no centralized notification scheme, and instead, reporting obligations vary widely across all 50 states. This complexity makes it harder to respond appropriately and swiftly to protect people in the event of a data breach. We believe this is an important issue and an area that is ripe for thoughtful regulation.

Question 4. With more than two billion monthly active users, Facebook is by far the largest social networking platform on the internet. Some have called Facebook a monopoly and claimed that Facebook has no true competition.

- If a Facebook user living in the United States wanted to switch to a different online social networking platform, what are the top ten alternative social networking platforms available? To the best of your knowledge, how many monthly active users does each attract?

Answer. In Silicon Valley and around the world, new social apps are emerging all the time. The average American uses eight different apps to communicate with their friends and stay in touch with people. There is a lot of choice, innovation, and activity in this space, with new competitors arising all the time. Facebook's top priority and core service is to build useful and engaging products that enable people to connect, discover and share through mobile devices and personal computers. Given its broad product offerings, Facebook faces numerous competitors, competing to attract, engage, and retain users, to attract and retain marketers, and to attract and retain developers who build compelling mobile and web applications. For instance, if you want to share a photo or video, you can choose between Facebook, DailyMotion, Snapchat, YouTube, Flickr, Twitter, Vimeo, Google Photos, and Pinterest, among many other services. Similarly, if you are looking to message someone, just to name a few, there's Apple's iMessage, Telegram, Skype, Line, Viber, WeChat, Snapchat, and LinkedIn—as well as the traditional text messaging services your mobile phone carrier provides. Equally, companies also have more options than ever when it comes to advertising—from billboards, print and broadcast, to newer platforms like Facebook, Spotify, Twitter, Google, YouTube, Amazon, or Snapchat. Facebook represents a small part (in fact, just 6 percent) of this $650 billion global advertising ecosystem and much of that has been achieved by helping small businesses—many of whom could never have previously afforded newspaper or TV ads—to cost-effectively reach a wider audience.

Question 5. Last week, legislation that I supported to combat online sex trafficking—the Allow States and Victims to Fight Online Sex Trafficking Act (FOSTA)—was signed into law. Facebook also supported that legislation.

- What has Facebook observed in terms of efforts to facilitate human trafficking on its platform, and what actions has Facebook taken in response?

Answer. Sex trafficking has no place on Facebook. Our Community Standards make it very clear that human trafficking and smuggling are against our policies. This is true across the platform. We remove content that threatens or promotes sexual violence, assault, or exploitation, including against minors, when we become aware of it. We have a team of professional investigators and work with agencies across the world that seek to identify and rescue victims and bring perpetrators to justice.

Facebook is committed to making our platform a safe place, especially for individuals who may be vulnerable. We have a long history of working successfully with governments to address a wide variety of threats to our platform, including child exploitation. When we learn of a situation involving physical abuse, child exploitation, or an imminent threat of harm to a person, we immediately report the situation to first responders or the National Center for Missing and Exploited Children (NCMEC).

Further, as part of official investigations, government officials sometimes request data about people who use Facebook. We have processes in place to handle these government requests, and we disclose account records in accordance with our terms of service and applicable law. We also have a global team that strives to respond within minutes to emergency requests from law enforcement.

Our relationship with NCMEC also extends to an effort that we launched in 2015 to send AMBER Alerts to the Facebook community to help find missing children. When police determine that a case qualifies for an AMBER Alert, the alert is issued by the NCMEC and distributed through the Facebook system with any available information, including a photograph of the missing child, a license plate number, and the names and descriptions of the child and suspected abductor. Law enforcement determines the range of the target area for each alert. We know the chances of finding a missing child increase when more people are on the lookout, especially in the critical first hours. Our goal is to help get these alerts out quickly to the people who are in the best position to help, and a number of missing children have been found through AMBER Alerts on Facebook.

Further, we work tirelessly to identify and report child exploitation images (CEI) to appropriate authorities. We identify CEI through a combination of automated and manual review. On the automated review side, we use image hashing to identify known CEI. On the manual review side, we provide in-depth training to content reviewers on how to identify possible CEI. Confirmed CEI is reported to the NCMEC, which then forwards this information to appropriate authorities. When we report content to the NCMEC, we preserve account information in accordance with applicable law, which can help further law enforcement investigations. We also reach out to law enforcement authorities in serious cases to ensure that our reports are received and acted upon.

Since 2015 we have proactively engaged with relevant NGOs working to safeguard girls and women from trafficking and violence to understand where we can do more. This included a number of roundtables on the topic of women's safety, including trafficking and prostitution. For example:

- *X-Industry Child Safety Hackathon:* In May 2016, we invited over 75 engineers from across industry, including Microsoft and Google, as well as from child safety NGOs, such as NCMEC, Thorn, and InHope, to the Facebook campus in San Francisco for the first-ever cross industry child safety hackathon to develop tools and products that enhance child online safety (read more at *https://www.wearethorn.org/blog/hackathon-creates-tech-solutions-child-safety/?utm_campaign=coschedule&utm_source=facebook_page&utm_medium=Thorn&utm_content=Hackathon%20Creates%20Tech%20Solutions%20for%20Child%20Safety*) . We again hosted the hackathon in 2017 and have now added the TechCoalition and Google as co-hosts to the event to expand its scope and reach. One of the prototypes that came out of the hackathon is a tool that enables people to match known photos of missing children against online trafficking ads.
- *Roundtable with leading organizations to share best practices and build network.* On October 24, 2017, we hosted our first anti-sex trafficking roundtable in Menlo Park. The roundtable was attended by representatives from law enforcement officials, government agencies and anti-trafficking non-governmental organizations. The focus of the roundtable was to allow participants to discuss

and share expertise, experience, and research. The Sex Trafficking Cross-functional Team will continue to collaborate with both our internal and external partners on the objectives, projects, and deliverables discussed at the roundtable.

We have created shortcuts on Facebook and Instagram to provide education and additional resources (developed in conjunction with the National Human Trafficking Resource Center) to people who search for terms related to sex trafficking. These terms have been provided by internal and external experts and when someone searches for them on Facebook, we will have a pop-up that reminds them sex trafficking is illegal and violates our policies and shares resources for getting help.

RESPONSE TO WRITTEN QUESTIONS SUBMITTED BY HON. CHRISTOPHER COONS TO MARK ZUCKERBERG

Question 1. In 2015, Facebook learned that Aleksandr Kogan sold users' data he obtained from an application to the political consulting firm Cambridge Analytica in violation of Facebook's terms of service. Facebook did not publicly disclose that Cambridge Analytica obtained this user data until 2018, after public reports that Kogan had improperly sold the data to Cambridge Analytica.

a. Why did you fail to tell the public until March 2018 that Kogan sold the data to Cambridge Analytica?

b. Who specifically at Facebook made the decision not to tell the public that millions of users' data was obtained by Cambridge Analytica without their consent?

c. Your announcement that at least 87 million users had their privacy violated came out only recently. In 2015, did you try to determine the universe of users whose privacy was violated?

d. How long have you known the number of affected users was in the millions?

Answer. When Facebook learned about Kogan's breach of Facebook's data use policies in December 2015, we took immediate action. The company retained an outside firm to assist in investigating Kogan's actions, to demand that Kogan and each party he had shared data with delete the data and any derivatives of the data, and to obtain certifications that they had done so. Because Kogan's app could no longer collect most categories of data due to changes in Facebook's platform, our highest priority at that time was ensuring deletion of the data that Kogan may have accessed before these changes took place. With the benefit of hindsight, we wish we had notified people whose information may have been impacted. Facebook has since notified all people potentially impacted with a detailed notice at the top of their newsfeed.

Question 2. In your testimony for the hearing, you noted, "In 2015, we learned from journalists at *The Guardian* that Kogan had shared data from his app with Cambridge Analytica."

a. Prior to learning this from *The Guardian,* what steps was Facebook taking to ensure that developers were not selling data to third parties in violation of the site's terms of service?

Answer. Since 2014, Facebook has proactively reviewed any app seeking to obtain extended permissions to data beyond a basic set of data, and it has rejected more than half of the apps seeking these permissions. Before we learned about the *Guardian* allegations and through today, Facebook's policies regarding third-party usage of its platform technologies have prohibited—and continue to prohibit—those third-party app developers from selling or licensing user data accessed from Facebook and from sharing any user data accessed from Facebook with any ad network, data broker or other advertising or monetization-related service. We take action on potential violations of our Platform Policies based on proactive review, external reports, and other signals.

b. Why did Facebook wait until eight months after *The Guardian*'s report about Cambridge Analytica to send a letter asking for certification that the data was deleted?

Answer. Facebook did not wait until eight months after *The Guardian*'s report about Cambridge Analytica to seek assurance that the data was deleted. Facebook contacted Cambridge Analytica the day the article was released. About one month later, on January 18, 2016, Cambridge Analytica assured Facebook in writing that it had deleted the data received from Kogan/GSR and that their server contained no backups of the data.

c. If it were not for *The Guardian*'s reporting, would you have learned that Kogan sold the data to Cambridge Analytica? If yes, how?

Answer. We learned from journalists at *The Guardian* that Kogan may have shared data from his app with Cambridge Analytica. We would have acted in response to any external report, user report, or other signal to investigate these allegations and take appropriate action.

d. It is likely that there will not always be a newspaper reporting on every application developer that improperly sells user data. Has Facebook ever proactively (*i.e.,* without being alerted by another party) learned about a similar violation of its terms of service—selling or transferring user data without consent to a third party—and if so, how? How many other such instances have you discovered?

Answer. We regularly take enforcement action against apps. For example, in 2017, we took action against about 370,000 apps, ranging from imposing certain restrictions to removal of the app from the platform.

As part of the app investigation and audit we announced in March, we have suspended 200 apps, pending a thorough investigation into whether they did in fact misuse any data. These apps relate to a handful of developers: Kogan, AIQ, Cube You, the Cambridge Psychometrics Center, and myPersonality, with many of the suspended apps being affiliated with the same entity. Many of these apps also appear to be "test" apps that were never released to the public, and therefore would not have acquired significant user data, although our investigation into these apps is ongoing.

Additionally, we have suspended an additional 14 apps, which were installed by around one thousand people. They were all created after 2014, after we made changes to more tightly restrict our platform APIs to prevent abuse. However, these apps appear to be linked to AIQ, which was affiliated with Cambridge Analytica. So, we have suspended them while we investigate further. Any app that refuses to take part in or fails our audit will be banned.

Question 3. Why did Facebook only recently suspend Cambridge Analytica's and Aleksandr Kogan's Facebook accounts when you knew about the illicit transfer of user data back in 2015?

a. Why did Facebook fail to take legal action back in 2015 when it learned from *The Guardian* that Kogan sold the data to Cambridge Analytica?

b. After Cambridge Analytica's acquisition of data came to Facebook's attention in 2015, did any policy or process change within your company in response? Please describe any such changes and when they occurred.

Answer. See Response to Question 1.

Question 4. In 2014, Facebook stopped allowing applications access to the profiles of a user's friends, but for applications like Aleksandr Kogan's, you still allowed access to friends' data for another year. Why did Facebook permit other applications continued access to that data for another year?

Answer. In April 2014, we announced that we would more tightly restrict our platform APIs to prevent abuse. At that time we made clear that existing apps would have a year to transition—at which point they would be forced (1) to migrate to the more restricted API and (2) be subject to Facebook's new review and approval protocols. A small number of developers asked for and were granted short-term extensions beyond the one-year transition period, the longest of which lasted several months. These extensions ended several years ago. A transition period of this kind is standard when platforms implement significant changes to their technology base and was necessary here to avoid disrupting the experience of millions of people. New apps that launched after April 30, 2014 were required to use our more restrictive platform APIs.

Question 5. Can you now confirm that Cambridge Analytica and its partners, AggregateIQ and Strategic Communications Laboratories, have deleted the Facebook data they received from Aleksandr Kogan? If not, why not?

a. Has Facebook ever attempted to prevent Cambridge Analytica from offering products or services that rely on or use the data it improperly obtained from Kogan?

b. Is there anything that will prevent Cambridge Analytica from offering products or services that rely on or use the illicitly acquired Facebook data in the 2018 and 2020 elections?

Answer. Facebook obtained written certifications from Kogan, GSR, and other third parties (including Cambridge Analytica and SCL) declaring that all data they had obtained, and any derivatives, was accounted for and destroyed. Based on recent allegations, we have reopened our investigation into the veracity of these certifications and have hired a forensic auditor to conduct a forensic audit of Cambridge Analytica's systems. We are currently paused on the audit at the request of the UK Information Commissioner's Office request, which is conducting a regulatory

investigation into Cambridge Analytica (based in the UK), and we hope to move forward with that audit soon.

We have suspended SCL/Cambridge Analytica from purchasing advertising on Facebook as well as removed the personal accounts of some of their officers.

Question 6. You wrote in your testimony that, in March 2018, Facebook hired a firm to conduct a forensic audit of Cambridge Analytica and Kogan. Why did Facebook wait until March of 2018 to conduct an audit of Cambridge Analytica's and Kogan's systems to ensure the data was destroyed, when the company has known for three years that the data was misappropriated?

Answer. Facebook knew about Cambridge Analytica in 2015, when Facebook banned Kogan's app from our platform and investigated what happened and what further action Facebook should take to enforce our Platform Policies. Facebook considered the matter closed after obtaining written certifications and confirmations from Kogan, GSR, Cambridge Analytica, and SCL declaring that all such data they had obtained was accounted for and destroyed.

We did not have any reason to affirmatively question the veracity of any of these certifications until March 2018, when we learned that questions had been raised concerning the accuracy of the certifications. Moreover, while Facebook's policies in place at the time allowed us to audit apps to ensure that they were safe and did not violate its terms, we had already terminated Kogan's app's access to Facebook (and there was no intention of considering its reinstatement). Accordingly, there were no ongoing concerns about the level of data that app could access or might access in the future.

Facebook, and Mr. Zuckerberg, became aware from media reporting in March 2018 that the certifications we received may not have been accurate. Facebook immediately banned Cambridge Analytica and SCL from purchasing advertisements on our services as well as removed the personal accounts of some of their officers.

Question 7. In an interview with CBS's *60 Minutes,* Aleksandr Kogan estimated that "tens of thousands" of application developers had similar access to their participants' friends' profiles.

a. Approximately how many other application developers had access to their users' friends' profiles, like Kogan?

Answer. Facebook is in the process of investigating all the apps that had access to large amounts of information, such as extensive friends data (if those friends privacy data settings allowed sharing), before we changed our platform policies in 2014—significantly reducing the data apps could access. Where we have concerns about individual apps, we are investigating them—and any app that either refuses or fails an audit will be banned from Facebook. To date thousands of apps have been investigated and around 200 have been suspended—pending a thorough investigation into whether they did in fact misuse any data.

These apps relate to a handful of developers: Kogan, AIQ, Cube You, the Cambridge Psychometrics Center, and myPersonality, with many of the suspended apps being affiliated with the same entity. Many of these apps also appear to be "test" apps that were never released to the public, and therefore would not have acquired significant user data, although our investigation into these apps is ongoing.

Additionally, we have suspended an additional 14 apps, which were installed by around one thousand people. They were all created after 2014, after we changed our platform to reduce data access. However, these apps appear to be linked to AIQ, which was affiliated with Cambridge Analytica. So, we have suspended them while we investigate further. Any app that refuses to take part in or fails our audit will be banned.

b. Has Facebook ever learned of an application developer other than Kogan transferring or selling user data without user consent and in violation of Facebooks terms of service to a third party?

Answer. The ability for app developers to share data entrusted to them is an industry-wide challenge, which impacts every major app platform. We will investigate all apps that had access to large amounts of data before the platform changes we announced in 2014, and among other things, analyze potentially suspicious activity from our analysis of logs and usage patterns by these apps. Where we have concerns, we will conduct an audit using internal and external experts and ban any developer that refuses to comply. If we identify misuses of data, our enforcement actions may include banning the app from our platform and pursuing legal action if appropriate.

Question 8. Have there been instances in which Facebook discovered misuse of user data by application developers in any way other than transferring or selling data without user consent?

a. If so, how many additional instances does Facebook currently know about?

b. Have you notified any users in these cases? If not, will you commit to doing so?

c. Will you commit to publicly announcing and notifying users of every future violation of Facebook's terms of service by application developers?

Answer. We are in the process of investigating every app that had access to a large amount of information before we changed our platform in 2014. The investigation process is in full swing, and it has two phases. First, a comprehensive review to identify every app that had access to this amount of Facebook data and to focus on apps that present reason for deeper investigation. And second, where we have concerns, we will conduct interviews, make requests for information (RFI)—which ask a series of detailed questions about the app and the data it has access to—and perform audits using expert firms that may include on-site inspections. We have large teams of internal and external experts working hard to investigate these apps as quickly as possible. To date thousands of apps have been investigated and around 200 apps have been suspended—pending a thorough investigation into whether they did in fact misuse any data. Where we find evidence that these or other apps did misuse data, we will ban them and let people know.

These apps relate to a handful of developers: Kogan, AIQ, Cube You, the Cambridge Psychometrics Center, and myPersonality, with many of the suspended apps being affiliated with the same entity. Many of these suspensions include apps that appear to be "test" apps that were never released to the public, and therefore would not have acquired significant user data, although our investigation into these apps is ongoing.

Additionally, we have suspended an additional 14 apps, which were installed by around one thousand people. They were all created after 2014, after we made changes to more tightly restrict our platform APIs to prevent abuse. However, these apps appear to be linked to AIQ, which was affiliated with Cambridge Analytica. So, we have suspended them while we investigate further. Any app that refuses to take part in or fails our audit will be banned.

We will commit to briefing your staff on future developments.

Question 9. The Guardian recently reported that Joseph Chancellor, former co-director of Aleksandr Kogan's company, Global Science Research (GSR), has been working as a quantitative social psychologist at Facebook since 2015. In an interview for CBS's *60 Minutes,* Kogan was asked whether Chancellor had anything to do with the study he did for Cambridge Analytica. He replied, "Yes. I mean, we did everything together."

a. Does Facebook continue to employ Chancellor, knowing since 2015 that he was involved in GSR's harvesting and sale of Facebook data to Cambridge Analytica? If so, why?

b. Facebook banned Aleksandr Kogan's account and required that he certify the user data he harvested was deleted. Did Facebook take similar actions against Chancellor? If not, why not?

Answer. We are investigating Mr. Chancellor's work with Kogan/GSR.

Question 10. Cambridge Analytica whistleblower Christopher Wylie testified to the U.K. House of Commons that Russian intelligence agencies easily could have put a key logger in Aleksandr Kogan's computer during his regular trips to Russia to get his psychological profiles of Americans. Is Facebook aware of whether Russia or other foreign governments accessed Kogan's data?

Answer. We are not aware of any evidence to suggest that Kogan shared data obtained through his app with Russia or other foreign governments, but our investigation is ongoing.

a. Is Facebook aware of any instances in which foreign governments accessed user data from third-party application developers?

Answer. We are in the process of investigating every app that had access to a large amount of information before we changed our Platform in 2014.

b. What steps is Facebook taking to ensure that foreign governments cannot access the private information of U.S. citizens held by application developers?

Answer. In April 2014, we announced that we would more tightly restrict our platform APIs to prevent abuse. At that time we made clear that existing apps would have a year to transition—at which point they would be forced (1) to migrate to the more restricted API and (2) be subject to Facebook's new review and approval protocols. A small number of developers asked for and were granted short-term extensions beyond the one-year transition period, the longest of which lasted several months. These extensions ended several years ago. A transition period of this kind is standard when platforms implement significant changes to their technology base and was necessary here to avoid disrupting the experience of millions of people. New

apps that launched after April 30, 2014 were required to use our more restrictive platform APIs. We required apps seeking additional categories of data to undergo proactive review by our internal teams. We rejected more than half of the apps seeking these permissions, including the second version of Kogan's app.

We review apps to ensure that the requested permissions clearly improve the user experience and that the data obtained is tied to an experience within the app. We conduct a variety of manual and automated checks of applications on the platform for Policy compliance, as well as random sampling. When we find evidence of or receive allegations of violations, we investigate and, where appropriate, employ a number of measures, including restricting applications from our platform, preventing developers from building on our platform in the future, and taking legal action where appropriate.

Recently, we announced a number of additional steps we're taking to address concerns raised by Kogan's app.

- *Review our platform.* We will investigate all apps that had access to large amounts of data before the platform changes we announced in 2014, and we will audit any app where we identify suspicious activity. If we identify misuses of data, we'll take immediate action, including banning the app from our platform and pursuing legal action if appropriate.
- *Tell people about data misuse.* We will tell people about apps that have misused their data. This includes building a way for people to know if their data might have been accessed via the app. Moving forward, if we remove an app for misusing data, we will tell everyone who used it.
- *Turn off access for unused apps.* If someone has not used an app within the last three months, we will turn off the app's access to their data.
- *Restrict Facebook Login data.* We are changing Login, so that the only data that an app can request without app review will include name, profile photo, and email address. Requesting any other data will require approval from Facebook. We will also no longer allow apps to ask for access to information like religious or political views, relationship status and details, custom friends lists, education and work history, fitness activity, book reading and music listening activity, news reading, video watch activity, and games activity. We will encourage people to manage the apps they use. We already show people what apps their accounts are connected to and allow them to control what data they've permitted those apps to use. But we're making it easier for people to see what apps they use and the information they have shared with those apps.
- *Reward people who find vulnerabilities.* We launched the Data Abuse Bounty program so that people can report to us any misuses of data by app developers.
- *Update our policies.* We have updated our terms and Data Policy to explain how we use data and how data is shared with app developers.

c. Is there a way for Facebook to affirmatively track Facebook data that application developers download from the platform such that you know when that data has been improperly accessed or transferred?

Answer See Response to Question 10, part b.

Question 11. Why did Facebook threaten *The Guardian* with legal action after it sought to publish an interview with former Cambridge Analytica employee Christopher Wylie? Has Facebook ever taken legal action against a current or former employee who attempted to, or did, expose violations of user agreements?

Answer. Facebook did not threaten to sue *The Guardian.* We sent *The Guardian* a letter to correct some facts in the article they sought to publish. Facebook supports vocal, independent journalism.

Question 12. Facebook sends employees or affiliates to work as consultants with campaigns to help shape digital strategy, content, and execution. Do you plan to embed such Facebook consultant embeds in major political campaigns in the 2018 and 2020 elections? If yes, what will Facebook instruct such consultant embeds about their responsibility to monitor for improper uses of Facebook user data or breaches of the Facebook user agreement?

Answer. We want all candidates, groups, and voters to use our platform to engage in elections. We want it to be easy for people to find, follow, and contact their elected representatives—and those running to represent them. That's why, for candidates across the political spectrum, Facebook offers the same levels of support in key moments to help campaigns understand how best to use the platform.

a. Were any of Facebook's consultant embeds in 2016 aware of the user data improperly acquired by Cambridge Analytica?

Answer. While our investigation is ongoing, our review indicates that Facebook employees did not identify any issues involving the improper use of Facebook data in the course of their interactions with Cambridge Analytica during the 2016 U.S. Presidential campaign.

b. Did Facebook consultant embeds work with Cambridge Analytica in shaping strategy for any U.S. campaigns in 2016?

Answer. In general, political data firms working on the 2016 campaign had access to Facebook's advertising support services, including technical support, and best practices guidance on how to optimize their use of Facebook.

Question 13. In 2011, Facebook entered into a binding consent decree with the FTC, in which it promised to get users' consent before sharing their data with third parties. Yet, as late as 2015, app developers had access to the Facebook profiles of the friends of users who downloaded their apps, without the friends' knowledge or consent. Why did Facebook permit this even after entering into the consent decree with the FTC?

a. In the consent decree, Facebook further agreed to report any unauthorized access to data to the FTC. Did Facebook ever report to the FTC that Cambridge Analytica accessed the profiles of at least 87 million Facebook users without Facebook's authorization or those users' consent?

b. If not, why not, and who made the decision that this did not have to be reported to the FTC?

Answer. We furnished extensive information to the FTC regarding the ability for users to port their Facebook data (including friends data that had been shared with them) with apps on Facebook's platform, as part of the FTC's investigation culminating in the July 27, 2012 Consent Order. The Consent Order memorializes the agreement between Facebook and the FTC and did not require Facebook to turn off or change the ability for people to port friends data that had been shared with them on Facebook to apps they used. Facebook voluntarily changed this feature of Platform in 2014, however.

Instead, and among other things, the consent order obligates Facebook not to misrepresent the extent to which it maintains the privacy or security of covered information (Section I), not to materially exceed the restrictions of a privacy setting that applies to nonpublic user information without affirmative express consent (Section II), and to implement a comprehensive privacy program that is subjected to ongoing review by an independent assessor (Sections IV and V). Facebook (i) accurately represented the operation of its developer Platform and the circumstances under which people could share data (including friends data) with developers at all times; (ii) honored the restrictions of all privacy settings that covered developer access to data (including settings that allowed people to turn off the ability of their friends to share their data with apps); and (iii) implemented a comprehensive privacy program build on industry-leading controls and principles, which has undergone ongoing review by an independent assessor approved by the FTC.

The Consent Order does not contain ongoing reporting obligations to the FTC of the sort suggested in this question. Moreover, Kogan was authorized to access all data that he obtained through Facebook's platform by the people who authorized his app, and no data was shared with Kogan relating to friends who had enabled settings preventing their data from being shared with apps by their friends.

Question 14. Last year, Facebook generated almost $40 billion in advertising revenues. How much is Facebook spending on data privacy and security?

a. How much is Facebook spending to ensure compliance with civil rights laws?

Answer. We do not have a single budget line-item for these efforts.

b. The NAACP, Muslim Advocates, the Leadership Conference, the Southern Poverty Law Center, and over a dozen other civil rights organizations asked for a third-party civil rights audit of Facebook's policies in October 2017. Will you commit to hiring an independent third party to conduct an audit focused on civil rights and privacy?

Answer. Relman, Dane & Colfax, a respected civil rights law firm, will carry out a comprehensive civil rights assessment of Facebook's services and internal operations. Laura Murphy, a national civil liberties and civil rights leader, will help guide this process—getting feedback directly from civil rights groups, like The Leadership Conference on Civil and Human Rights, and help advise Facebook on the best path forward.

Question 15. Does Facebook use artificial intelligence to analyze content posted by users in order to assist in the creation of targeted advertisements? How many individuals are involved in reviewing advertisements that are targeted using personal information?

Answer. Facebook does not analyze the content of photos or text in users' posts or messages to target ads to them using AI or otherwise. Instead, there are a few primary ways that we personalize the ads and sponsored content for people on Facebook, based on:

- *Information from people's use of Facebook.* When people use Facebook, they can choose to share things about themselves like their age, gender, hometown, or interests. They can also click or like posts, Pages, or articles. We use this information to understand what users might be interested in and hopefully show them ads that are relevant. If a bike shop comes to Facebook wanting to reach female cyclists in Atlanta, we can show their ad to women in Atlanta who liked a Page about bikes. People can always see the "interests" assigned to them in their ad preferences, and if they want, remove them.
- *Information that an advertiser shares with us (or "custom audiences").* In this case, advertisers bring us the customer information so they can reach those people on Facebook. These advertisers might have people's e-mail address from a purchase users made, or from some other data source. If we have matching e-mail addresses, we can show those people ads from that advertiser (although we cannot see the e-mail addresses which are sent to us in hashed form, and these are deleted as soon as we complete the match). In ad preferences people can see which advertisers with their contact information are currently running campaigns—and they can click the top right corner of any ad to hide all ads from that business.
- *Information that websites and apps send to Facebook.* Some of the websites and apps people visit may use Facebook tools to make their content and ads more relevant, if people consent to let Facebook show them ads based on data from third-party partners. For example, if an online retailer is using Facebook Pixel, they can ask Facebook to show ads to people who looked at a certain style of shoe or put a pair of shoes into their shopping cart. If users don't want this data used to show them ads, they can turn it off in ad preferences.
- *Facebook also offers Lookalike Audiences.* Advertisers creating a Lookalike Audience choose a source audience (which could include a custom audience as described above, people who have opened or completed a form in lead ads on Facebook, people who have interacted with the advertiser's Facebook page or its Instagram profile). Facebook then identifies common qualities of the people in the source audience (*e.g.,* demographic information or information about their interests), and then identifies people who are similar to them (on the basis of the common signals identified in the source audience), without sharing this information with the advertiser.

We have thousands of people whose job it is to help review ads for compliance with our policies. We recently announced that we are hiring thousands of additional reviewers this year.

Question 16. Would it be possible to create a one-click way for a Facebook user to opt out of targeted advertising?

a. Why did you decide not to offer that option to users?

b. Will you commit to offering that option in the future?

c. Have you considered creating a one-click way for a user to prevent Facebook from collecting and storing data beyond what individual users elect to post?

Answer. Users can't opt out of seeing ads altogether because selling ads are what keep Facebook free, but they do have different options to control how their data can and can't be used to show them ads. They're all found in ad preferences, which allows users to turn off the use of all data collected from partners off Facebook to target ads.

Users can also decide which of their profile fields they want used for ad targeting in the Information section under "About you." Users can remove themselves from interests under "Your interests" and categories under "Your categories."

Question 17. What do Facebook and its subsidiary companies consider "private" information that is not collected or used for advertising purposes? Is there any content that users provide or post that Facebook does not analyze or review for advertising purposes?

Answer. As explained in our Data Policy, we collect three basic categories of data about people: (1) data about things people do and share (and who they connect with) on our services, (2) data about the devices people use to access our services, and (3) data we receive from partners, including the websites and apps that use our business tools. Our Data Policy provides more detail about each of the three categories.

We use data from each of the categories described above to obtain these interests and to personalize every aspect of our services, which is the core value we offer and the thing that makes Facebook services unique from other online experiences. This includes selecting and ranking relevant content, including ads, posts, and Page recommendations, to cite but a few examples.

For example, we use the data people provide about their age and gender to help advertisers show ads based on those demographics but also to customize the pronouns on our site and deliver relevant experiences to those users.

We use data about things people do on Facebook, such as the Pages they like, to associate "interests" with their accounts, so we can rank posts relating to those interests higher in NewsFeed, for example, or enable advertisers to reach audiences—*i.e.,* groups of people—that share those interests. For example, if a person has liked Pages about baseball, we might associate them with interests called "baseball" or "sports."

We use data from devices (such as location data) to help advertisers reach people in particular areas. For example, if people have shared their device locations with Facebook or checked into a specific restaurant, we can show them organic posts from friends who have been in that location or we can show them ads from an advertiser that wants to promote its services in their area or from the restaurant.

We also help advertisers reach people who have given the advertiser their contact information or who have used the advertiser's website or app. For example, advertisers can send us a hashed list of e-mail addresses of people they would like to reach on Facebook. If we have matching e-mail addresses, we can show those people ads from that advertiser (although we cannot see the e-mail addresses which are sent to us in hashed form, and these are deleted as soon as we complete the match).

Again, for people who are new to Facebook, we may have minimal data that we can use to personalize their experience, including their News Feed, their recommendations and the content (organic and sponsored) that they see. For people who have used our services for longer, we likely have more data, but the amount of data will depend on the nature of that use and how they have used our controls.

In addition to general controls—such as Activity Log—we provide controls that specifically govern the use of data for ads. Through Ad Preferences, people see and control things like: (1) their "interests," which are keywords associated with a person based on activities such liking Pages and clicking ads; (2) their "behaviors" (which we also call "categories"), which generally reflect how, when and where they connect to Facebook; and (3) the advertisers that are currently showing them ads based on the person's contact information, based on the person's previous use of the advertiser's website or app, or based on a visit to the advertiser's store. People also can choose whether we use information about their activities on websites and apps off of Facebook to show them ads through Facebook, and whether we can use their Facebook advertising interests to show them ads off of Facebook. People's use of these controls will, of course, affect the data we use to show them ads.

Question 18. If a user leaves Facebook and affirmatively deletes his/her account, do you destroy his/her data?

a. What, if any, information is retained after a user profile is deleted?

b. If any data is retained by Facebook, what is that data used for?

Answer. In general, when a user deletes their account, we delete things they have posted, such as their photos and status updates, and they won't be able to recover that information later. (Information that others have shared about them isn't part of their account and won't be deleted.)

There are some limited exceptions to these policies: For instance, information can be accessed and preserved for an extended period when it is the subject of a legal request or obligation, governmental investigation, or investigations of possible violations of our terms or policies, or otherwise to prevent harm. We also retain information from accounts disabled for terms violations for at least a year to prevent repeat abuse or other term violations.

Question 19. At your hearing before the House Committee on Commerce and Energy, when asked by Representative Gene Greene if you would "commit today that Facebook will extend the same protections to Americans that Europeans users will receive under the GDPR," you replied: "Yes Congressman, we believe that everyone around the world deserves good privacy controls. We've had a lot of these privacy controls in place for years, the GDPR requires us to do a few more things, and we're going to extend that to the world." However, *Reuters* recently reported that, before the GDPR becomes effective in the EU in May, you plan to move non-European users' data—including profile data on 1.5 billion users from Africa, Asia, Australia, and Latin America—from Ireland to Silicon Valley in order to "reduce exposure" to the GDPR (available at *https://www.reuters.com/article/us-facebook-privacy-eu*

-exclusive/exclusive-facebook-to-put-1-5-billion-users-out-of-reach-of-new-eu-privacy-law-idUSKBN1HQ00P).

a. Can you confirm that the reason you are moving 1.5 billon users' data is to avoid unnecessary exposure to the GDPR?

Answer. No, that is not the reason. The change referred to in this question involves the legal entity with which Facebook users contract when they use the service, which changed in some jurisdictions as a part of the most recent updates to our Terms of Service and Data Policy. This change did not impact people who live in the United States, who contract with Facebook, Inc. under both our new and old policies.

The substantive protections in our user agreements offered by Facebook Ireland and Facebook, Inc. are the same. However, there are certain aspects of our Facebook Ireland Data Policy that are specific to legal requirements in the GDPR—such as the requirement that we provide contact information for our EU Data Protection Officer (DPO) or that we identify the "legal bases" we use for processing data under the GDPR. Likewise, our Facebook Ireland terms and Data Policy address the lawful basis for transferring data outside the EU, based on legal instruments that are applicable only to the EU.

We are also looking to be more responsive to regional norms and legal frameworks going forward, and want to have the flexibility to work with local regulators, which is possible with this new model. At the same time, we are changing the provisions in our Facebook, Inc. terms in our user agreements outside the United States to allow people in other countries to file lawsuits against Facebook in their home country, rather than in courts in the U.S. This transition was part of a continued effort to be locally responsive in countries where people use our services.

b. Do you agree that such a move fails to show your willingness to apply stronger privacy controls and practices to all of your users?

Answer. No. See the answer above. In addition, the controls and settings that Facebook is enabling as part of GDPR are already available to other users around the world, including settings for controlling our use of face recognition on Facebook and for controlling our ability to use data we collect off Facebook Company Products to target ads. We also provide the same tools for access, rectification, erasure, data portability and others to users in the U.S. and rest of world that we provide in Europe, and many of those tools (like our Download Your Information tool, Ads Preferences tool, and Activity Log) have been available globally for many years.

c. Is your response to Representative Greene at your hearing, that you were "going to extend [the things required by the GDPR] to the world," consistent with Facebook's actions to relocate massive amounts of user data outside of the EU following your hearings?

Answer. We are not relocating people's data. To enable people to access Facebook globally and communicate with people throughout the world, we maintain data centers in multiple locations around the world. We typically store people's information in multiple data centers, and that is not changing. We are instead changing the entity that provides the service for users outside of Europe and North America to Facebook, Inc., for the reasons set forth above. We are offering the same controls and settings to people everywhere.

Question 20. Facebook continues to find Russian trolls operating on your platform. At your hearing, you stated, "just last week, we were able to determine that a number of Russian media organizations that were sanctioned by the Russian regulator were operated and controlled by this Internet Research Agency." Hate groups thrive on Facebook even though your policies prohibit hate speech and glorifying violence. Fake duplicate profiles of real users frequently appear on the site in spite of Facebook policy prohibiting them. This recently happened to me, and I had to alert Facebook in order to have this false profile taken down. Why does Facebook shift the burden to its users to flag inappropriate content—is it not Facebook's job to protect its users?

Answer. Facebook does not "shift the burden" to users to flag inappropriate content, though we encourage people to report posts to help us find and take action on inappropriate content. Advances in technology, including in artificial intelligence, machine learning, and computer vision mean that we can now remove bad content faster, get to more content, and increase the capacity of our review team. It has taken time to develop this software—and we're constantly pushing to improve it. We do this by analyzing specific examples of bad content that have been reported and removed to identify patterns of behavior. These patterns can then be used to teach our software to proactively find other, similar problems. But understanding the context of speech, for example, often requires human eyes—is something hateful, or is it being shared to condemn hate speech or raise awareness about it? We've started

using technology to proactively detect something that might violate our policies, starting with certain languages such as English and Portuguese. Our teams then review the content so what's OK stays up, for example someone describing hate they encountered to raise awareness of the problem.

a. Is Facebook's artificial intelligence technology capable of automatically flagging fake profiles?

Answer. Claiming to be another person violates our Community Standards, and we want to make it harder for anyone to be impersonated on our platform. Users can also report accounts that are impersonating them. We've developed several techniques to help detect and block this type of abuse. At the time someone receives a friend request, our systems are designed to check whether the recipient already has a friend with the same name, along with a variety of other factors that help us determine if an interaction is legitimate. Further, we recently announced new features that use face recognition technology that may help detect when someone is using another user's image as their profile photo—which helps stop impersonation. This is an area we're continually working to improve so that we can provide a safe and secure experience on Facebook.

b. Is there currently any automated system in place for flagging fake profiles or fake news articles at Facebook?

Answer. We block millions of fake account attempts each day as people try to create them thanks to improvements in machine learning and artificial intelligence. We are also working hard to stop the spread of false news. To reduce the spread of false news, we remove fake accounts and disrupt economic incentives for traffickers of misinformation. We also use various signals, including feedback from our community, to identify potential false news. In countries where we have partnerships with independent third-party fact-checkers, stories rated as false by those fact-checkers are shown lower in News Feed. If Pages or domains repeatedly create or share misinformation, we significantly reduce their distribution and remove their advertising rights.

c. If yes, do Facebook employees review every such potentially fake profile or news article that these systems flag?

Answer. Not every fake account that has been disabled is reviewed as the volume is simply too great (Facebook took action on approximately 583 million fake accounts in the first three months of 2018). But our engineers carefully test and retest the accuracy of the policies and rules they implement to identify and disable fake accounts.

d. Do Facebook employees manually search for fake content, or is the function of flagging fake or inappropriate content left solely to users and automated systems?

Answer. See Response to previous question (Question 20, part c).

Question 21. Special Counsel Robert Mueller's indictment of 13 Russian individuals and three Russian companies states that the Russians have engaged in "'information warfare against the United States of America' through fictitious U.S. personas on social media platforms," including Facebook. As a U.S. company, do you have an obligation to prevent your platform from being used as a weapon against our democracy?

a. What are you doing to prevent Facebook from being used for information warfare in the 2018 election and beyond?

Answer. In the run-up to the 2016 elections, we were focused on the kinds of cybersecurity attacks typically used by nation states, for example phishing and malware attacks. And we were too slow to spot this type of information operations interference. Since then, we've made important changes to prevent bad actors from using misinformation to undermine the democratic process.

This will never be a solved problem because we're up against determined, creative, and well-funded adversaries. But we are making steady progress. Here is a list of the 10 most important changes we have made:

1. Ads transparency. Advertising should be transparent: users should be able to see all the ads an advertiser is currently running on Facebook, Instagram and Messenger. And for ads with political content, we've created an archive that will hold ads with political content for seven years—including information about ad impressions and spend, as well as demographic data such as age, gender, and location. People in Canada and Ireland can already see all the ads that a Page is running on Facebook—and we're launching this globally in June.

2. Verification and labeling. Every advertiser will now need confirm their ID and location before being able to run any ads with political content in the U.S. All ads with political content will also clearly state who paid for them.

3. Updating targeting. We want ads on Facebook to be safe and civil. We thoroughly review the targeting criteria advertisers can use to ensure they are consistent with our principles. As a result, we removed nearly one-third of the targeting segments used by the IRA. We continue to allow some criteria that people may find controversial. But we do see businesses marketing things like historical books, documentaries or television shows using them in legitimate ways.

4. Better technology. Over the past year, we've gotten increasingly better at finding and disabling fake accounts. We now block millions of fake accounts each day as people try to create them—and before they've done any harm. This is thanks to improvements in machine learning and artificial intelligence, which can proactively identify suspicious behavior at a scale that was not possible before—without needing to look at the content itself.

5. Action to tackle fake news. We block millions of fake account attempts each day as people try to create them thanks to improvements in machine learning and artificial intelligence. We are also working hard to stop the spread of false news. To reduce the spread of false news, we remove fake accounts and disrupt economic incentives for traffickers of misinformation. We also use various signals, including feedback from our community, to identify potential false news. In countries where we have partnerships with independent third-party fact-checkers, stories rated as false by those fact-checkers are shown lower in News Feed. If Pages or domains repeatedly create or share misinformation, we significantly reduce their distribution and remove their advertising rights.

6. Significant investments in security. We're doubling the number of people working on safety and security from 10,000 last year to over 20,000 this year. We expect these investments to impact our profitability. But the safety of people using Facebook needs to come before profit.

7. Industry collaboration. Recently, we joined 34 global tech and security companies in signing a TechAccord pact to help improve security for everyone.

8. Information sharing and reporting channels. In the 2017 German elections, we worked closely with the authorities there, including the Federal Office for Information Security (BSI). This gave them a dedicated reporting channel for security issues related to the Federal elections.

9. Tracking 40+ elections. In recent months, we've started to deploy new tools and teams to proactively identify threats in the run-up to specific elections. We first tested this effort during the Alabama Senate election, and plan to continue these efforts for elections around the globe, including the U.S. midterms. Last year we used public service announcements to help inform people about fake news in 21 separate countries, including in advance of French, Kenyan and German elections.

10. Action against the Russia-based IRA. In April, we removed 70 Facebook and 65 Instagram accounts—as well as 138 Facebook Pages—controlled by the IRA primarily targeted either at people living in Russia or Russian-speakers around the world including from neighboring countries like Azerbaijan, Uzbekistan, and Ukraine. The IRA has repeatedly used complex networks of inauthentic accounts to deceive and manipulate people in the U.S., Europe and Russia—and we don't want them on Facebook anywhere in the world.

We are taking steps to enhance trust in the authenticity of activity on our platform, including increasing ads transparency, implementing a more robust ads review process, imposing tighter content restrictions, and exploring how to add additional authenticity safeguards.

b. Have you made any attempt to identify Russian political advertisements or troll accounts that are not associated with the Internet Research Agency?

Answer. Facebook has conducted a broad search for evidence that Russian actors, not limited to the IRA or any other specific entity or organization, attempted to interfere in the 2016 election by using Facebook's advertising tools. We found coordinated activity that we now attribute to the IRA, despite efforts by these accounts to mask the provenance of their activity. We have used the best tools and analytical techniques that are available to us to identify the full extent of this malicious activity, and we continue to monitor our platform for abuse and to share and receive information from others in our industry about these threats.

Question 22. Do you have the technology or capability to detect when a foreign entity is attempting to buy a political ad?

Answer. Now all election and issue ads on Facebook and Instagram in the U.S. must be clearly labeled—including a "Paid for by" disclosure from the advertiser at the top of the ad. This will help ensure that people can see who is paying for the

ad—which is especially important when the Page name doesn't match the name of the company or person funding the ad. This also meets the commitments we made back in October 2017 to increase the transparency of the election-related ads people see on Facebook.

When people see that label, it means the person running the ad went through the authorization process and verified his or her identity and location. We believe this new level of transparency is good for people, and it will allow journalists, researchers, NGOs and others to hold campaigns, candidates and organizations accountable for the ads they create. And all people on Facebook, no matter where they live, will also be able to access and review a searchable archive that will house these ads for seven years from the day they run. More information about our transparency efforts can be found at our recent Newsroom posthere: *https://newsroom.fb.com/news/2018/05/hard-questions-political-ads*.

Moreover, Facebook's Statement of Rights and Responsibilities (the terms that govern all use of our services) prohibit using Facebook to do anything that is unlawful, misleading, or malicious. In addition, advertisers must comply with Facebook's Advertising Policies, including acknowledging that they are responsible for understanding and complying with all applicable laws and regulations. Therefore, violating the Federal Election Campaign Act also violates our terms.

We also have processes designed to identify inauthentic and suspicious activity and we also maintain a sanctions compliance program to screen advertisers and paid app developers. Facebook's denied party screening protocol involves checking paid app developers and advertisers against applicable denied party listings. Those screened remain in an on-going monitoring portfolio and are screened against changes to applicable denied party listings. Moreover, our payments subsidiaries file Suspicious Activity Reports on developers of certain apps as appropriate. However, like other offline and online companies, Facebook has limited insight into the use of shell corporations or other sophisticated structures that may disguise the true buyer. In addition, the general challenge of attributing online activities to specific governments or organizations is widely recognized in the intelligence and law enforcement communities.

a. If so, do you have any procedures to inform U.S. enforcement agencies when a foreign entity is attempting to buy a political ad or when it may be taking other steps to interfere in an election?

Answer. In general, we have a long history of working successfully with the DOJ, the FBI, and other law enforcement to address a wide variety of threats to our platform. We deeply respect and value the seriousness, diligence, and support of those organizations, and we would welcome their partnership as we work to address this specific threat. We are particularly encouraged by the FBI's creation of a task force dedicated to addressing election interference and we are actively working with that newly-formed body. This is a new kind of threat, and we believe that we will need to work together—across industry and between industry and government—to be successful.

b. What trends have you discovered with respect to the rate at which foreign entities are attempting to interfere in our elections? Is this tactic becoming more prevalent over time?

Answer. See Response to Question 21, part b.

RESPONSE TO WRITTEN QUESTIONS SUBMITTED BY HON. MAZIE HIRONO TO MARK ZUCKERBERG

Collection of Personal Data of Non-Facebook Users

Question 1. We asked you many questions at our hearing about what rights Facebook users have or should have to know what personal data of theirs Facebook has, to know who their data is shared with, and to have effective control over the use of their personal data. At a hearing the next day in the House of Representatives, you testified that Facebook also collects "data of people who have not signed up for Facebook." These are people who are not on Facebook and have had no ability to opt in or out of sharing their personal data. In many if not most instances, they may not know that Facebook has collected this data.

In response to criticism of this revelation, Facebook told the press that it has no plans to build a tool that would disclose to non-users that their data had been collected. Facebook's statement stated that "[t]his kind of data collection is fundamental to how the Internet works," and "standard to how the Internet works" and suggested that people use "browser or device settings to delete cookies," which are one of the ways in which Facebook and others track people on the internet.

I have serious concerns that this answer is incomplete and dismissive of the concerns. You said at the House hearing that this kind of 3rd-party data collection was done for "security purposes." But that answer also seems incomplete and not consistent with Facebook's later statement that this is "standard to how the Internet works." Let me give you an opportunity to clarify.

a. Why do you collect this third party personal data from non-Facebook users?

b. How do you collect this third party personal data from non-Facebook users? Please be specific, including whether and how you use "cookies" and other hidden trackers.

c. How do you use the personal data you collect from non-Facebook users? What do you use it to measure or analyze?

d. Do you use the personal data of non-Facebook users to target ads? If so, how is that consistent with your testimony at the hearing that such data is collected for "security purposes"?

e. Does collecting cookies from any websites with Facebook "like" buttons or otherwise tracking the data of non-Facebook users serve any "security purposes"? If so, how? If not, why did you testify that the collection of such date was for "security purposes"?

f. How do you store personal data you collect from non-Facebook users? Do you ever delete this data?

Answer. When people visit apps or websites that feature our technologies—like the Facebook Like or Comment button—our servers automatically log (i) standard browser or app records of the fact that a particular device or user visited the website or app (this connection to Facebook's servers occurs automatically when a person visits a website or app that contains our technologies, such as a Like button, and is an inherent function of Internet design); and (ii) any additional information the publisher of the app or website chooses to share with Facebook about the person's activities on that site (such as the fact that a purchase was made on the site). This is a standard feature of the Internet, and most websites and apps share this same information with multiple different third-parties whenever people visit their website or app. For example, the Senate Commerce Committee's website shares information with Google and its affiliate DoubleClick and with the analytics company Webtrends. This means that, when a person visits the Committee's website, it sends browser information about their visit to each one of those third parties. More information about how this works is available at *https://newsroom.fb.com/news/2018/04/data-off-facebook/*.

When the person visiting a website featuring Facebook's tools is not a registered Facebook user, Facebook does not have information identifying that individual, and it does not create profiles for this individual.

We use the browser and app logs that apps and websites send to us—described above—in the following ways for non-Facebook users. First, these logs are critical to protecting the security of Facebook and to detecting or preventing fake account access. For example, if a browser has visited hundreds of sites in the last five minutes, that's a sign the device might be a bot, which would be an important signal of a potentially inauthentic account if that browser then attempted to register for an account. Second, we aggregate those logs to provide summaries and insights to websites and apps about how many people visit or use their product, or use specific features like our Like button—but without providing any information about a specific person. We do not create profiles for non-Facebook users, nor do we use browser and app logs for non-Facebook users to show targeted ads from our advertisers to them or otherwise seek to personalize the content they see. However, we may take the opportunity to show a general ad that is unrelated to the attributes of the person or an ad encouraging the non-user to sign up for Facebook.

Question 2. According to the Princeton Web Transparency & Accountability Project (WebTAP), Facebook trackers are used on about 25 percent of the top million websites. Gabriel Weinberg, CEO and Founder of DuckDuckGo, an Internet privacy company, wrote recently on FastCompany.com that Facebook uses these trackers to create "shadow profiles" even of non-Facebook users based on their browsing history. However, Facebook said in a press statement that it does not create databases on non-users by combining web-browsing history with uploaded contacts.

a. Can you confirm that you do not create such databases of non-users or clarify in what ways you collect and use the personal data of non-users that you collect?

b. Can you specify whether you use tracking of non-Facebook users' personal data to create "shadow profiles" of them and/or any other type of profile of them and, if so, how are these profiles used?

c. Do you believe that Americans who use the Internet have a right to know they are being tracked and profiled by Facebook and other companies like Google? Do you believe American have the right to have access to the contents of those profiles?

d. Given that non-users of Facebook have not had the opportunity to consent at all to Facebook's collection of their data, let alone its use, do you believe they should be given the opportunity to "opt in" before their personal data is tracked and captured?

Answer. Facebook does not create profiles or track website visits for people without a Facebook account. See response to Question 1 for more detail.

Adopting the EU's Model for Personal Data Protection

Question 3. On May 25, just a few weeks from now, the European Union will put into effect its new General Data Protection Regulation, or GDPR. Under that system, the concept of ownership over personal data is almost completely upside down from what we have in America. In Europe, where data protection is a fundamental right, consent to use that information can only be given if it is clear, affirmative and unambiguous. Owners of data may withdraw their consent at any time, and companies and organizations must notify the EU of serious data breaches as soon as possible, and not wait years, as happens here.

The week before our hearing, you told reporters that you intend to make the same controls and settings required under the GDPR everywhere. However, when you were asked about applying these new regulations in the U.S., you were much more vague, committing only that applying these European regulations here in the U.S. is "worth discussing." I want to start having that discussion now.

a. Will you commit to making the setting and controls required by GDPR available everywhere, including in America? If not, why not, and what privacy controls and settings will you make available here?

Answer. The controls and settings that Facebook is enabling as part of GDPR are available to people around the world, including settings for controlling our use of face recognition on Facebook and for controlling our ability to use data we collect off Facebook Company Products to target ads. We recently began providing direct notice of these controls and our updated terms to people around the world (including in the U.S.), allowing people to choose whether or not to enable or disable these settings or to consent to our updated terms. We provide the same tools for access, rectification, erasure, data portability, and others to people in the U.S. and the rest of world that we provide in Europe, and many of those tools (like our Download Your Information tool, ad preferences tool, and Activity Log) have been available globally for many years.

b. Will users in this country have the right to data portability, where they will be able to transfer their personal data from Facebook if they choose?

Answer. See Response to Question 3(a).

c. At the hearing many Senators discussed with you the need for Facebook users to be notified promptly when their data has been hacked. You told Senator Klobuchar you though 72 hours for notification "makes sense to [you]." Can you commit to a 72 hour timeline for notification?

Answer. One of the challenges with notification in the United States is that there is no Federal breach notification law, which means that notification technically requires reaching out to 50 different state regulators under a patchwork of different frameworks. While we would support a short time period for notification in the United States, this would need to be part of a centrally managed Federal scheme that would make this process efficient and manageable. In Europe, for example, we are required to notify our lead supervisory authority—the Irish Data Protection Commissioner—within 72 hours of a data breach that poses a risk to the rights and freedoms of data subjects, not every single Member State's data protection authority. Moreover, the GDPR only requires notification to people in cases where there is a high risk of harm to an individual resulting from the breach *and* where the data controller is unable to mitigate that harm through subsequent measures that prevent continued access to the data, etc. GDPR thus creates incentives for companies to work with a lead regulator and to mitigate harm to people, reserving notification to people for cases where there is no other means to avoid a high risk of harm to people. This reflects a responsible and thoughtful evaluation of the potential risks to people resulting from public notification, which would have the effect of publicizing a breach that could then be exploited by bad actors (who might not otherwise know about it). The regulatory notification requirement ensures there is appropriate oversight in a specific situation.

d. Will you treat what Article 9 of the GDPR calls "Special Categories" of personal data, such as data revealing, among other things, racial or ethnic origin, religious beliefs, and genetic data, according to the strict EU standards?

Answer. We are prompting people in Europe and in the United States to go through an engagement flow that educates them about data they have shared on their profiles that constitutes "special categories of personal data" under GDPR (such as information they choose to include in their profile like religious and political views). This experience gives people—including both people in Europe and people in the U.S.—the ability to delete this information from their profile through in-line controls.

e. Will Facebook users who gave consent to share their data be able to withdraw that consent at any time?

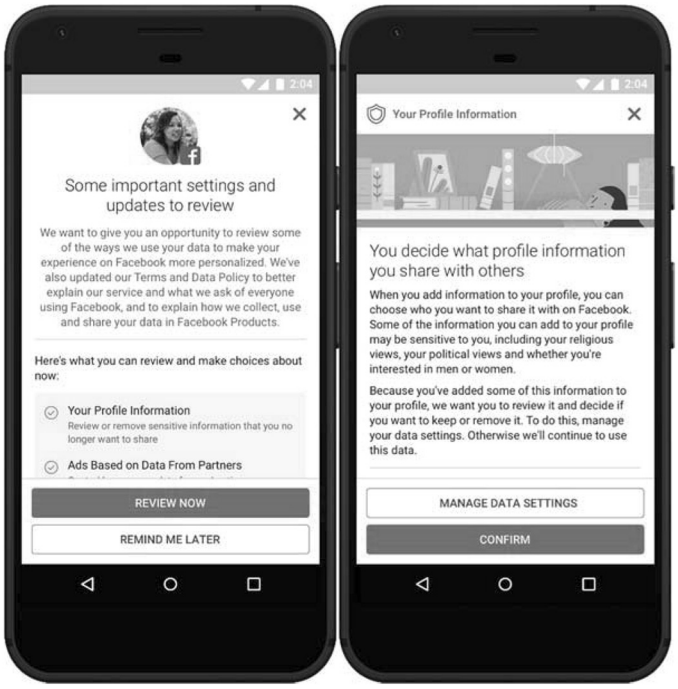
Answer. Yes, by visiting Facebook Settings. For sharing of specific pieces of information, such as a Facebook post or a field in a person's Facebook profile, people also have the ability to delete this information or change the audience who is eligible to see it.

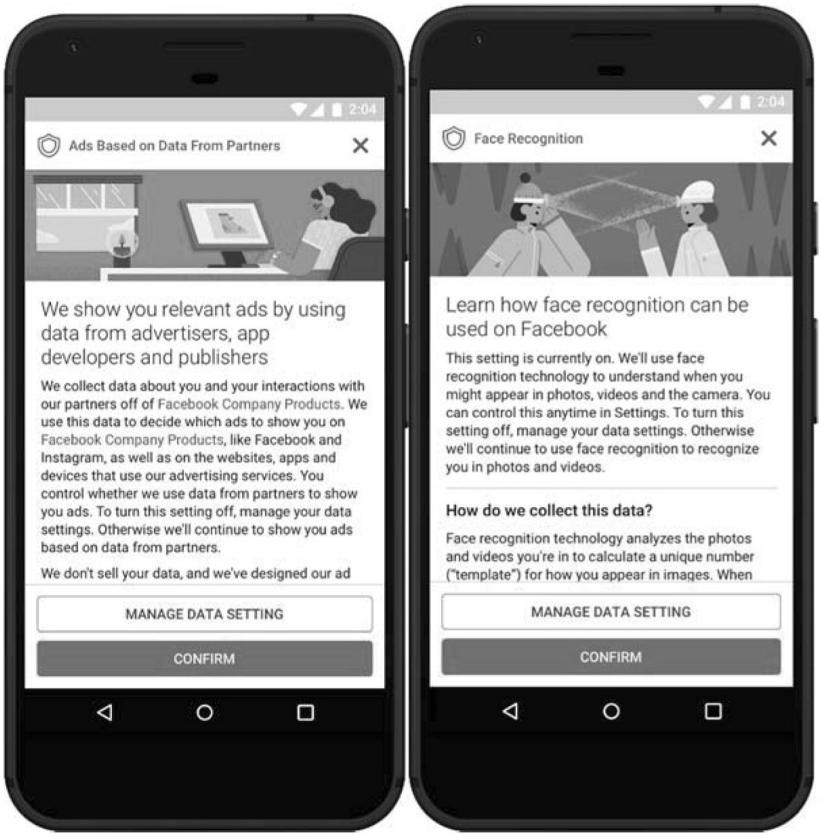
f. Would Facebook's collection of the personal data of non-users be permissible under these GDPR regulations, which require affirmative notice and consent?

Answer. GDPR does not require consent for most uses of personal information, and instead, recognizes that many uses of data are necessary to provide a service or within a company's legitimate interests or the public interest, etc. We agree that different levels of consent or notice are appropriate depending on the type of information or contemplated use at issue. The GDPR does not differentiate between users and non-users, and indeed, many online or digital services around the world do not require registration or distinguish between "users" and "non-users" before collecting or logging data, such as browser logs of people who visit their website.

g. Considering that these regulations go into effect in less than a month, can you produce to the Committee the language that European users of Facebook will be presented with on May 25?

Answer. Yes, here are screenshots of the consent flows being provided in Europe:





Discriminatory Targeting of Facebook Ads

Question 4. I asked you several questions about whether Facebook is following its own stated policy of forbidding Facebook ads that excluded audiences for the ads on the basis of race, gender, family status, sexual orientation, disability or veteran status. These are all categories prohibited by Federal law in housing and employment law. Yet, in October 2016, journalists at Pro Publica revealed that it was possible to buy Facebook ads that excluded these audiences. Even though Facebook announced in February 2017 that it would no longer allow such ads, a year later Pro Publica found they could still place them. They also found ads for employment that excluded age groups employers weren't interested in targeting, also a violation of Federal law.

I appreciated your sincerity in telling me and other Senators that it is "against [Facebook] policies to have any ideas that are discriminatory." I also appreciate your candor, after describing the need for more active screening, in admitting that policing discriminatory targeting is "a work in progress." I want to ask you about the path forward in enforcing your policy, and your assessment of Facebook's capacity to handle these problems and the legal concerns they raise without outside enforcement.

a. At the hearing you cited your anti-discrimination policy. Yet, it has been well over a year since Facebook announced it would no longer allow ads that used discriminatory, and in some cases illegal, targeting and you admit that you still need to develop better tools. How do you measure and assess that you efforts to enforce your own anti-discrimination policies are working?

b. The story from Pro Publica suggests little if any progress has been made, even though during the whole period of time your policy against discrimination was your

policy, and you explicitly banned the purchase of ad engaging in discriminatory targeting over a year ago. Recognizing this is a "work in progress," what does improvement look like to you? What does complying with your policy look like to you?

c. What accountability is there for failure to comply with your policy against discriminatory targeting?

d. In addition to your existing screening of ads and flags raised by the community that you follow-up on with your team, you suggested that Facebook needs "to develop more AI tools that can more proactively identify those types of content and do that kind of filtering up front." What are your plans for developing and timeline for deploying these tools, and when do you expect to see a measurable progress the elimination of discriminatory targeting?

e. Is there a way for the public to verify that you have made progress or are we just expected to trust you?

Answer. Our Terms and Advertising Policies have long emphasized our prohibition on the use of Facebook's platform to engage in wrongful discrimination. Starting in late 2016, we began implementing additional protections for the people who use Facebook. Specifically, we set out to help better educate advertisers about our policies against discrimination and relevant Federal and state laws, and to help prevent the abuse of our tools. First, we updated our Advertising Policies applicable to all advertisers and advertisements to strengthen our prohibition against discrimination, and we added a section to provide advertisers with anti-discrimination educational resources from government agencies and civil rights groups. Second, we implemented technical measures aimed at better protecting users from wrongful discrimination by advertisers that offer housing, employment and credit opportunities. We continue to work to improve these measures.

We are continuing to evaluate the targeting options we make available to advertisers. This work involves consultation with key stakeholders outside the company, including with policymakers, regulators, civil rights experts, and consumer advocates. The decision to remove targeting options is not something we take lightly: as many of these stakeholders have pointed out, targeting is a key mechanism for forging meaningful connections between people and organizations on Facebook.

One recent example illustrates the challenge of getting this work right. Earlier this year, we eliminated the ability to target people based on the "interested in" field that people can add to their Facebook profiles. People can indicate that they are interested in men, women, or both, and some consider the field to be a place where people can indicate their sexual orientation. After receiving feedback from a range of stakeholders, we eliminated the ability to target based on this field. Although some groups applauded the decision, others criticized it, noting that it would now be harder to reach certain groups.

We also are working to provide more in-product education about advertisers' obligations under our non-discrimination policy, and anticipate that this education will be more detailed and will be presented to a broader range of advertisers than our current education. Finally, we will soon launch View Ads, a feature that will enable anyone to see all of the ads an advertiser is currently running by visiting the advertiser's Facebook Page. This level of transparency is unprecedented among advertising platforms, and we believe it will further our efforts to combat discrimination by giving people the opportunity to see ads regardless of whether they are in the target audience.

We have focused on measures that are designed to prevent advertisers from misusing our tools to place discriminatory housing, credit and employment ads, including: requiring such advertisers to certify their compliance with our Advertising Policies and with relevant anti-discrimination laws and prophylactically removing advertisers' ability to use certain categories of information to target their audience. Some of these measures are proactive, such as the classifiers we use to detect when an advertiser is attempting to run a housing, credit, or employment ad. Facebook rejects ads from advertisers who do not certify compliance. We also recently launched automated tools to proactively identify racist or offensive content and hate speech in ads.

In addition, Facebook conducts an automated review of ads to ensure that they do not assert or imply personal attributes in violation of our Advertising Policies. Ads that violate this policy are rejected. Advertisers can appeal these rejections. Understanding that we might not be able to prevent every misuse of our ad tools, we encourage users to report offensive ads to Facebook. Ads that violate our Advertising Policies are removed when we become aware of them. We also anticipate that the View Ads tool—which, as described above, will allow people to see all the ads an advertiser is currently running—will encourage people to report more ads to us, and will therefore enhance our efforts to curtail misuse of our tools.

Consumer Protection for Facebook Users

Question 5. American consumers rightfully expect that they can take part in the market for goods and services while being protected from certain kinds of harm. The government makes sure that our food and drugs aren't tainted. We have laws that make sure advertising in print or on TV and radio doesn't contain lies. We demand transparency and honesty from banks and stock brokers.

Yet, for Americans using Facebook, there is almost a total lack of these kinds of protections. And when Americans suffer harm, there is no accountability for Facebook. We are expected to hand over our most vital personal information with no control over how it is used or misused, and we are told this is the cost of "connection" and of being part of the Facebook "community". I know that since some of the worst breaches of trust were discovered you've been talking about the steps you are taking to do better.

a. Why should we leave it up to you to protect America's Facebook consumers?

b. Do you think they are any less deserving of their government's protection than milk drinkers or detergent buyers or home buyers seeking a mortgage? What makes your business different?

Answer. Facebook is generally not opposed to regulation but wants to ensure it is the right regulation. We are already regulated in many ways—for example, under the Federal Trade Commission Act—and we are subject to ongoing oversight by the FTC under the terms of a 2011 consent order. Facebook has inherent incentives to protect its customers' privacy and address breaches and vulnerabilities. Indeed, the recent discovery of misconduct by an app developer on the Facebook platform clearly hurt Facebook and made it harder for us to achieve our social mission. As such, Facebook is committed to protecting our platform from bad actors, ensuring we are able to continue our mission of giving people a voice and bringing them closer together. We are also actively building new technologies to help prevent abuse on our platform, including advanced AI tools to monitor and remove fake accounts. We have also significantly increased our investment in security, employing more than 15,000 individuals working solely on security and content review and planning to increase that number to over 20,000 by the end of the year. We have also strengthened our advertising policies, seeking to prevent discrimination while improving transparency.

Question 6. When users sign up for services on Facebook, they are asked for consent to use their personal data in certain ways. But it's typically in the form of pages of small print that pop up on the screen that few people bother to read. And as these terms of services change over time or as users sign up for new services, they are asked to click a box next to yet more pages of small print. The Pew Research Center tells us that about 52 percent of Internet users believe that "when a company posts a privacy policy, it ensures that the company keeps confidential all the information it collects on users."

Do you believe this is a reasonable expectation of people who sign up to use Facebook? Should it be?

Answer. We believe that it's important to communicate with people about the information that we collect and how people can control it. This is why we work hard to provide this information to people in a variety of ways: in our Data Policy, and in Privacy Basics, which provides walkthroughs of the most common privacy questions we receive. Beyond simply disclosing our practices, we also think it's important to give people access to their own information, which we do through our Download Your Information and Access Your Information tools, Activity Log, and Ad Preferences, all of which are accessible through our Privacy Shortcuts tool. We also provide information about these topics as people are using the Facebook service itself.

Facebook seeks, as much as possible, to put controls and information in context within its service. While "up front" information like that contained in the terms of service are useful, research overwhelmingly demonstrates that in-product controls and education are the most meaningful to people and the most likely to be read and understood. On-demand controls are also important, and we recently redesigned our entire settings menu on mobile devices from top to bottom to make things easier to find. We also created a new Privacy Shortcuts menu where people can control their data in just a few taps, with clearer explanations of how our controls work. The experience is now clearer, more visual, and easy to find.

Improving people's understanding of how digital services work is an industry-wide challenge that we are highly committed to addressing. That's why, over the last 18 months, we've run a global series of design workshops called "Design Jams," bringing together experts in design, privacy, law and computer science to work collaboratively on new and innovative approaches. These workshops have run in Paris, London, Dublin, Berlin, Sao Paolo, Hong Kong, and other cities, and included global

regulators and policymakers. At these workshops, expert teams use "people centric design" methods to create innovative new design prototypes and experiences to improve transparency and education in digital services. These workshops inform Facebook's constantly-improving approach.

In recognition of the need for improved approaches to data transparency across all digital services, working with partners from academia, design, and industry we recently launched TTC Labs, a design innovation lab that seeks to improve user experiences around personal data. TTC Labs is an open platform for sharing and innovation and contains insights from leading experts in academia, design, and law, in addition to prototype designs from the Design Jams, template services and open-source toolkits for people-centric design for transparency, trust, and control of data. Working collaboratively, and based on open-source approaches, TTC Labs seeks to pioneer new and more people-centric best practices for people to understand how their data is used by digital services, in ways that they find easy to understand and control.

Facebook is highly committed to improving people's experience of its own services as well as investing in new innovations and approaches to support improvements across the industry.

Advertising Revenue Model and Facebook's Mission

Question 7. At the hearing and in recent interviews you have defended Facebook's approach to generating advertising revenue by targeting ads towards users. You proudly said that a model based on adverting is the only rational way to make Facebook accessible to all people. In response to Apple CEO Tim Cook saying he wouldn't have gotten himself into a situation like the one you and Facebook find yourselves in, you talked a lot about ways that Facebook shows it cares about its users. You defended your model as the best way to connect everyone.

a. But is an advertising based model really the only way to make Facebook accessible to all people, or is it the only way to do so while making massive profits?

Answer. Like many other free online services, we sell advertising space to third parties. Doing so enables us to offer our services to consumers for free. This is part of our mission to give people the power to build community and bring the world closer together. To build a secure product with extensive infrastructure that connects people across continents and culture, we need to make sure everyone can afford it. Advertising lets us keep Facebook free, which ensures it remains affordable for everyone.

Separately, our core service involves personalizing all content, features, and recommendations that people see on Facebook services. No two people have the same experience on Facebook or Instagram, and they come to our services because they expect everything they see to be relevant to them. If we were not able to personalize or select ads or other content based on relevance, this would fundamentally change the service we offer on Facebook—and it would no longer be Facebook.

We maintain our commitment to privacy by not telling advertisers who users are or selling people's information to anyone. That has always been true. We think relevant advertising and privacy are not in conflict, and we're committed to doing both well.

b. Isn't there a better way that balances the making of profits with stronger privacy protections, and shouldn't it be our role in Congress to make sure we are keeping that balance?

Answer. Privacy is at the core of everything we do, and our approach to privacy starts with our commitment to transparency and control—to helping people understand how their data is collected and used, and to giving them meaningful controls.

Question 8. Facebook's stated mission is "to give people the power to build community and bring the world closer together."

a. How is this mission consistent with your business model of finding ways to extract value from the personal data of users?

Answer. See Response to Question 7(a).

b. Doesn't the gross misuse of users' data without their consent to better target them with fake news undermine this mission by devaluing and dividing the community?

Answer. We believe targeted advertising creates value for people and advertisers who use Facebook. Being able to target ads to the people most likely to be interested in the products, service or causes being advertised enables businesses and other organizations to run effective campaigns at reasonable prices. This efficiency has particularly benefited small businesses, which make up the vast majority of the six million active advertisers on Facebook. That said, we are keenly aware of the concerns

about the potential of our tools to be abused. That is why we are investing heavily in improving the security and integrity of our platform.

c. What happens the next time you have a business reason to again compromise the personal data of users, or at least look the other way?

Answer. We do not have a "business reason" to compromise the personal data of users; we have a business reason to protect that information. Our mission is to build community and bring the world closer together, but it is not enough to just connect people—we have to make sure those connections are positive. If people's experiences are not positive—if we fail to maintain their trust—they will not use our services.

Irish Elections

Question 9. On May 25, 2018, there will be a referendum conducted in Ireland to determine whether there will be changes in abortion laws. Is Facebook willing to implement full transparency of political ads that they have accepted have targeted Irish voters, together with any information they hold on the person or organizations who paid to promote the content?

Answer. As of April 25, we added Ireland to our pilot program for the first phase of our transparency efforts—the View Ads tool. This has enabled Irish Facebook users to see all of the ads every page is running on Facebook targeting users in Ireland at the same time. We also announced on May 8 that we would begin rejecting ads related to the referendum if run by advertisers based outside of Ireland.

RESPONSE TO WRITTEN QUESTIONS SUBMITTED BY HON. CORY BOOKER TO MARK ZUCKERBERG

Question 1. In 2016, ProPublica revealed that advertisers could use "ethnic affinity" marketing categories to potentially discriminate against Facebook users in the areas of housing, employment, and credit, in violation of Federal law. While you committed in November 2016 to "build tools to detect and automatically disable the use of ethnic-affinity marketing for certain types of ads," a year later ProPublica found that the system you built was still letting housing ads through without applying the new restrictions. It was chalked up to a "technical failure." You then opted for system where advertisers self-certify that they are complying with Federal law and Facebook's antidiscrimination policy, but in fact just last month, several fair housing organizations filed a lawsuit against Facebook in the S.D.N.Y. alleging discrimination in housing advertising based not just on race, but also on disability, gender, and familial status. According to the lawsuit, the most recent ad buys were still occurring just weeks ago in late February 2018.

a. Is a self-certification model the strongest way to safeguard against discrimination?

Answer. Our Terms and Advertising Policies have long emphasized our prohibition on the use of Facebook's platform to engage in wrongful discrimination. Starting in late 2016, we began implementing additional protections for the people who use Facebook. Specifically, we set out to help better educate advertisers about our policies against discrimination and relevant Federal and state laws, and to help prevent the abuse of our tools. First, we updated our Advertising Policies applicable to all advertisers and advertisements to strengthen our prohibition against discrimination, and we added a section to provide advertisers with antidiscrimination educational resources from government agencies and civil rights groups. Second, we implemented technical measures aimed at better protecting users from wrongful discrimination by advertisers that offer housing, employment and credit opportunities. Specifically, when we identify one of these types of ads, we require the advertiser to certify that it is complying with our anti-discrimination policy and with applicable law. We reject thousands of ads a day where the advertiser fails to certify.

b. Would it be better to not serve ads in certain categories (housing/credit/employment) at all?

Answer. We have heard concerns about third party advertisers misusing these tools to engage in wrongful discrimination with respect to ads for housing, credit, and employment by targeting people based on the protected characteristics outlined in your questions. Based on feedback we have received from our community, and from policymakers, regulators, civil rights experts, and consumer advocates, we have limited the targeting options we offer for such advertisements that relate to protected classes as follows:

- We do not offer targeting based on race, religion, disability, sexual orientation, or gender identity.

- We do not offer targeting based on national origin, but we do have segments composed of "ex-pats"—people who used to live in particular countries (and may or may not be from these countries originally).
- We do permit some targeting based on family status (*e.g.,* people who are parents), but we generally do not permit advertisers to exclude people from their audiences based on family status. Please note, however, that in limited cases and for the purpose of running ads that are not related to housing, employment or credit, we are re-enabling the ability of advertisers to exclude people from their audiences based on family status but are reviewing this as a targeting option.
- Like other major ad platforms, we enable targeting based on age and gender.
- We offer targeting options—called "interests" and "behaviors"—that are based on people's activities on Facebook, and when, where and how they connect to the Internet (such as the kind of device they use and their mobile carrier). These options do not reflect people's personal characteristics, but we still take precautions to limit the potential for advertisers to misuse them. For example, we do not create interest or behavior segments that suggest the people in the segment are members of sensitive groups such as particular races, ethnicities, or religions. We therefore would not create an interest segment called "Muslims," because it could be misunderstood to enable an advertiser to reach people based on their religious beliefs.
- We also offer what we call the multicultural affinity segments, which are groups of people whose activities on Facebook suggest they may be interested in content related to the African American, Asian American, or Hispanic American communities. (For example, if a person "likes" Facebook Pages with the words "African American" in them or likes Pages for Historically Black Colleges and Universities, that person may be included in the African American multicultural segment.) As we explain to advertisers in our tools, these segments are based on people's activities on Facebook, not on race or ethnicity (which categories Facebook does not enable people to even include on their profiles).
- We have gone even further when it comes to using the "exclude" feature in our ads tools. This feature is designed to help advertisers refine their audiences by, for example, excluding people who are already interested in their products. But we recognize that permitting exclusions could, in some circumstances, raise the risk that an advertiser would engage in wrongful discrimination. For that reason, many of the targeting audiences that advertisers can choose to include in the group eligible to see their ad are not available for exclusion. For example, while we believe it is important that organizations be able to affirmatively reach people in the multicultural affinity segments, advertisers are not able to exclude people from their audiences based on the multicultural affinity segments.
- We also recently added a notice below the "exclude" field that reminds advertisers of their obligations under our non-discrimination policy as well as under relevant applicable law in a persistent manner when they create their advertisements and define their audiences.
- In early 2017, we launched machine learning tools (called "classifiers") that were intended to automatically identify, once an ad was entered into our systems, employment, credit, and housing ads. We built these classifiers so that when one of these kinds of ads was identified, we could take two actions that would make it harder for advertisers to misuse our tools.

c. Given your inability to fix something as straightforward as discriminatory housing ads, why should Congress trust Facebook's ability to target and reduce suspicious election activity?

Answer. These industry-wide problems are not easy to solve, but we are committed to doing better by implementing the steps outlined throughout this document.

d. How does Facebook prevent advertisers from using their own data to segment users by race or other protected categories using Facebook's Custom Audiences feature?

Answer. See Response to Question 1, part c.

Question 2. In responding to a November 2016 class action lawsuit against Facebook for discrimination in housing, employment, and credit, Facebook moved to dismiss the complaint on the basis that the plaintiffs were not injured.

a. Do you believe that people of color who are not recruited for various economic opportunities are harmed by not hearing about those opportunities?

Answer. We have Community Standards that prohibit hate speech, bullying, intimidation, and other kinds of harmful behavior. We hold advertisers to even stricter advertising policies to protect users from things like discriminatory ads. We don't want advertising to be used for hate or discrimination, and our policies reflect that. For example, we make it clear that advertisers may not discriminate against people based on personal attributes such as race, ethnicity, color, national origin, religion, age, sex, sexual orientation, gender identity, family status, disability, and medical or genetic condition. We educate advertisers on our anti-discrimination policy, and in some cases—including when we detect that an advertiser is running a housing ad—we require advertisers to certify compliance with our anti-discrimination policy and anti-discrimination laws.

Question 3. A 2016 investigation by the ACLU of California revealed that another app developer, Geofeedia, was using data from Facebook and other platforms to help law enforcement monitor the activities of peacefully protesting civilians of color. In response, Facebook changed its policy to prohibit any developers from facilitating the surveillance of Facebook users.

a. You have endorsed Black Lives Matter and expressed sympathy after Philando Castile's killing, which was broadcast on Facebook Live. Despite this, why should communities of color trust Facebook has sufficiently addressed this surveillance issue?

b. Is simply changing the language of your terms of service enough? Have you taken any other steps to prevent another Geofeedia from attempting something similar?

Answer. In March 2017, we added language to our Facebook and Instagram platform policies to more clearly explain that developers cannot use data obtained from us to provide tools that are used for surveillance. Our previous policy limited developers' use of data but did not explicitly mention surveillance. We found out that some developers created and marketed tools meant for surveillance, took action, and we clarified our policy.

RESPONSE TO WRITTEN QUESTIONS SUBMITTED BY HON. KAMALA HARRIS TO MARK ZUCKERBERG

Follow-up Questions Never Answered

At the hearing, I raised a series of questions for which you did not have answers. Please respond to those questions, which include:

Question 1. Whether Facebook can track users' browsing activity even after the user has logged off of Facebook?

Answer. When people visit apps or websites that feature our technologies—like the Facebook Like or Comment button—our servers automatically log (i) standard browser or app records of the fact that a particular device or user visited the website or app (this connection to Facebook's servers occurs automatically when a person visits a website or app that contains our technologies, such as a Like button, and is an inherent function of Internet design); and (ii) any additional information the publisher of the app or website chooses to share with Facebook about the person's activities on that site (such as the fact that a purchase was made on the site). This is a standard feature of the Internet, and most websites and apps share this same information with multiple different third-parties whenever people visit their website or app. For example, the Senate Commerce Committee's website shares information with Google and its affiliate DoubleClick and with the analytics company Webtrends. This means that, when a person visits the Committee's website, it sends browser information about their visit to each one of those third parties. More information about how this works is available at *https://newsroom.fb.com/news/2018/04/data-off-facebook/*.

When the person visiting a website featuring Facebook's tools is not a registered Facebook user, Facebook does not have information identifying that individual, and it does not create profiles for this individual.

We use the browser and app logs that apps and websites send to us—described above—in the following ways for non-Facebook users. First, these logs are critical to protecting the security of Facebook and to detecting or preventing fake account access. For example, if a browser has visited hundreds of sites in the last five minutes, that's a sign the device might be a bot, which would be an important signal of a potentially inauthentic account if that browser then attempted to register for an account. Second, we aggregate those logs to provide summaries and insights to websites and apps about how many people visit or use their product, or use specific features like our Like button—but without providing any information about a spe-

cific person. We do not create profiles for non-Facebook users, nor do we use browser and app logs for non-Facebook users to show targeted ads from our advertisers to them or otherwise seek to personalize the content they see. However, we may take the opportunity to show a general ad that is unrelated to the attributes of the person or an ad encouraging the non-user to sign up for Facebook.

When the individual is a Facebook user, we are also able to use this information to personalize that individual's experiences on Facebook, whether or not the individual is logged out, but we will not target ads to users relying on this information unless they allow this in their privacy settings. We do not sell or share this information with third-parties.

Question 2. Whether Facebook can track your activity across devices even when you are not logged into Facebook?

Answer. See Response to Question 1.

Question 3. Who are Facebook's biggest competitors?

Answer. In Silicon Valley and around the world, new social apps are emerging all the time. The average American uses eight different apps to communicate with their friends and stay in touch with people. There is a lot of choice, innovation, and activity in this space, with new competitors arising all the time. Facebook's top priority and core service is to build useful and engaging products that enable people to connect, discover, and share through mobile devices and personal computers. Given its broad product offerings, Facebook faces numerous competitors, competing to attract, engage, and retain users, to attract and retain marketers, and to attract and retain developers who build compelling mobile and web applications. For instance, if users want to share a photo or video, they can choose between Facebook, DailyMotion, Snapchat, YouTube, Flickr, Twitter, Vimeo, Google Photos, and Pinterest, among many other services. Similarly, if people are looking to message someone, just to name a few, there's Apple's iMessage, Telegram, Skype, Line, Viber, WeChat, Snapchat, and LinkedIn—as well as the traditional text messaging services their mobile phone carrier provides. Equally, companies also have more options than ever when it comes to advertising—from billboards, print, and broadcast, to newer platforms like Facebook, Spotify, Twitter, Google, YouTube, Amazon, or Snapchat. Facebook represents a small part (in fact, just 6 percent) of this $650 billion global advertising ecosystem and much of that has been achieved by helping small businesses—many of whom could never have previously afforded newspaper or TV ads—to cost-effectively reach a wider audience.

Question 4. Whether Facebook may store up to 96 categories of users' information?

Answer. Your question likely references a *Washington Post* article that purported to identify "98 data points that Facebook uses to target ads to you." The article was based on the writer's use of the tool that allows advertisers to select the audience that they want to see their ads. Anyone on Facebook can see the tool and browse the different audiences that advertisers can select.

The "data points" to which the article refers are not categories of information that we collect from everyone on Facebook. Rather, they reflect audiences into which at least some people on Facebook fall, based on the information they have provided and their activity. For example, the article lists "field of study" and "employer" as two of the "data points" that can be used to show ads to people. People can choose to provide information about their field of study and their employer in profile fields, and those who do may be eligible to see ads based on that information—unless they have used the controls in Ad Preferences that enable people to opt out of seeing ads based on that information. The same is true of the other items in the list of 98.

Further, the specific number of categories that are used to decide what ads a person will see vary from person to person, depending on the interests and information that they have shared on Facebook, how frequently they interact with ads and other content on Facebook, and other factors. Any person can see each of the specific interests we maintain about them for advertising by visiting Ads Preferences, which lets people see what interests we use to choose ads for them—and to edit or delete these interests. We also provide more detailed information about how we use data to decide what ads to show to people in our "About Facebook Ads" page, at *https://www.facebook.com/ads/about*.

Please note, however, that (as the article explains) many of these refer to "Partner Categories"—audiences that are offered by third-party data providers. We announced in April that we would stop offering this kind of targeting later this year.

Question 5. Whether you knew Dr. Kogan's terms of service?

Answer. Facebook has developed an automated system for checking that all apps had terms of service and data policies. In performing such checks, however, Facebook does not examine the content of the developers' terms and policies because app developers act as independent third parties with regard to the data they obtain;

they determine the purposes for which, and the manner in which, that data is processed. Our understanding is that this is consistent with the practices of other online and mobile platforms, which generally enable developers on their platforms to provide access to the developers' terms and policies in their app stores, but do not proactively review the substance of those policies.

Although developers act as independent third parties with regard to the data users share with them, all apps on the Facebook Platform must comply with our user data policies, Community Standards, Platform Policies, and Ad Guidelines. Our Platform policy also contains a number of enforcement provisions which apply after an app has been reviewed and approved. Facebook has several teams dedicated to detecting, escalating, investigating, and combating violations of its policies, including schemes to improperly access, collect, or exploit user data. The Developer Operations Policy Enforcement team looks for policy violations and either brings developers into compliance or removes them from the platform, and the Developer Operations Review team conducts an upfront review of apps to confirm proper use of advanced permissions.

Question 6. Whether you knew that Dr. Kogan could sell or transfer data?

Answer. Kogan was not permitted to sell or transfer data to third-parties for the purposes he did. In doing so, Kogan and his company violated Facebook's Platform Policies, which explicitly prohibit selling or licensing user data accessed from Facebook and from sharing any user data accessed from Facebook with any ad network, data broker, or other advertising or monetization-related service.

Scope of Data Collection

The core of Facebook's business model is the commodification of personal user data. This data culling and packaging is a complex endeavor, but the crux of it is simple—Facebook collects user data, categorizes it into demographic buckets, and works with advertising companies to target ads.

There are two realms of data collection—user-generated data (*e.g.* data input by the user such as name, gender, etc.) and platform-generated data (*e.g.* IP addresses, searches, and likes).

Question 1. Please answer, for the record, the following with a simple yes or no response. Does Facebook collect and permanently store:

a. Usernames?

Answer. Yes, Facebook collects a user's Facebook URL (*e.g.,* username or vanity for your account). Users can view the vanity URL in their Timeline URL. They can change their usernames via Settings.

b. Reported gender?

Answer. Yes, Facebook collects information regarding the gender a user added to the About section of their Timeline.

c. Reported address?

Answer. Yes, Facebook collects information regarding a user's current address or any past addresses they chose to include on their account.

d. Reported school affiliation?

Answer. Yes, Facebook collects information regarding any information a user added to Education field in the About section of your Timeline. Users can download Education information, as well as other information associated with their Facebook accounts, through our Download Your Information tool. We also recently introduced Access Your Information—a secure way for people to access and manage their information, such as posts, reactions, comments, and things they've searched for. Users can go here to delete anything from their timelines or profiles that they no longer want on Facebook.

If someone adds this information to their profile, they can later choose to delete it. If they do so, we will remove it from our site and delete it in accordance with our Data Policy.

e. Reported employment?

Answer. Yes, Facebook collects any current information a user has added to Work in the About section of their Timeline. They can download Work information, as well as other information associated with their Facebook account, through our Download Your Information tool. We also recently introduced Access Your Information—a secure way for people to access and manage their information, such as posts, reactions, comments, and things they've searched for. Users can go here to delete anything from their timelines or profiles that they no longer want on Facebook.

If someone adds this information to their profile, they can later choose to delete it. If they do so, we will remove it from our site and delete it in accordance with our Data Policy.

f. Reported political affiliation?

Answer. Yes, Facebook collects any information a user added to Political Views in the About section of Timeline. Users can download Political Views information, as well as other information associated with their Facebook accounts, through our Download Your Information tool. We also recently introduced Access Your Information—a secure way for people to access and manage their information, such as posts, reactions, comments, and things they've searched for. Users can go here to delete anything from their timelines or profiles that they no longer want on Facebook.

If someone adds this information to their profile, they can later choose to delete it. If they do so, we will remove it from our site and delete it in accordance with our Data Policy.

We recently began to prompt people on Facebook who have added a political affiliation to their profiles to review this information and decide whether they want to keep it on their profiles. More information about these prompts is available at *https://newsroom.fb.com/news/2018/05/pardon-the-interruption/*.

g. Every friend in a user's network?

Answer. Yes, Facebook collects a list of a user's friends. Users can download a list of their friends, as well as other information associated with their Facebook accounts, through our Download Your Information tool. We also recently introduced Access Your Information—a secure way for people to access and manage their information, such as posts, reactions, comments, and things you've searched for. Users can go here to delete anything from their timelines or profiles that they no longer want on Facebook.

If someone adds this information to their profile, they can later choose to remove a friend relationship. If they do so, we retain the fact that the friend relationship was removed in order to properly display privacy-protected content (for example, to avoid showing Friends-only information to people who previously had access) and for other purposes related to protecting the safety and privacy of people on Facebook.

h. Every friend ever deleted from a user's network?

Answer. Yes, Facebook collects information regarding people a user has removed as friends. Users can download deleted friend information, as well as other information associated with their Facebook account, through our Download Your Information tool. We also recently introduced Access Your Information—a secure way for people to access and manage their information, such as posts, reactions, comments, and things they've searched for. Users can go here to delete anything from their timelines or profiles that they no longer want on Facebook.

i. Every ad ever clicked on?

Answer. Yes, Facebook collects information regarding dates, times, and titles of ads clicked, although the retention period is limited. Users can download information about ads clicked, as well as other information associated with their Facebook accounts, through our Download Your Information tool. Through Ad Preferences, people see and control things like: (1) their "interests," which are keywords associated with a person based on activities such liking Pages and clicking ads; (2) their "behaviors" (which we also call "categories"), which generally reflect how, when, and where they connect to Facebook; and (3) the advertisers that are currently showing them ads based on the person's contact information, based on the person's previous use of the advertiser's website or app, or based on a visit to the advertiser's store. People also can choose whether we use information about their activities on websites and apps off of Facebook to show them ads through Facebook, and whether we can use their Facebook advertising interests to show them ads off of Facebook. People's use of these controls will, of course, affect the data we use to show them ads.

j. Every IP address ever used when logging into Facebook?

Answer. Facebook automatically logs IP addresses where a user has logged into their Facebook account. Users can download a list of IP addresses where they've logged into their Facebook accounts, as well as other information associated with their Facebook accounts, through our Download Your Information tool, although this list won't include all historical IP addresses as they are deleted according to a retention schedule.

k. Every "like"?

Answer. Yes, Facebook collects posts, photos, or other content a user has liked; likes on their own posts, photos, or other content; and likes they've made on sites off of Facebook. Users can manage the content and information they share when they use Facebook, including "likes," through the Activity Log tool. We also recently introduced Access Your Information—a secure way for people to access and manage their information, such as posts, reactions, comments, and things they've searched

for. Users can go here to delete anything from their timelines or profiles that they no longer want on Facebook.

If someone chooses to Like content on Facebook, they can later choose to remove that like. If they do so, we will remove it from our site and delete it in accordance with our Data Policy.

l. Every status change?

Answer. Yes, Facebook collects status updates a user has posted. Users can download status updates, as well as other information associated with their Facebook accounts, through our Download Your Information tool, and they can also manage the content and information they share when they use Facebook, including status updates, through the Activity Log tool. We also recently introduced Access Your Information—a secure way for people to access and manage their information, such as posts, reactions, comments, and things they've searched for. Users can go here to delete anything from their timelines or profiles that they no longer want on Facebook.

If someone adds this information to their profile, they can later choose to delete it. If they do so, we will remove it from our site and delete it in accordance with our Data Policy.

m. Every search of another person on Facebook?

Answer. Yes, Facebook collects searches a user has made on Facebook. Users can manage the content and information they share when they use Facebook, including searches, through the Activity Log tool. We also recently introduced Access Your Information—a secure way for people to access and manage their information, such as posts, reactions, comments, and things they've searched for. Users can go here to delete anything from their timeline or profile that they no longer want on Facebook.

When a user searches for something on Facebook, they can access and delete that query from within the search history in their Activity Log at any time, but the log of that search is deleted after 6 months.

Question 2. Assuming the above is not exhaustive, please list all types of data Facebook collects or otherwise acquires.

Answer. As explained in our Data Policy, we collect three basic categories of data about people:

(1) data about things people do and share (and who they connect with) on our services;

(2) data about the devices people use to access our services; and

(3) data we receive from partners, including the websites and apps that use our business tools.

As far as the amount of data we collect about people, the answer depends on the person. People who have only recently signed up for Facebook have usually shared only a few things—such as name, contact information, age, and gender. Over time, as people use our products, we receive more data from them, and this data helps us provide more relevant content and services. That data will fall into the categories noted above, but the specific data we receive will, in large part, depend on how the person chooses to use Facebook. For example, some people use Facebook to share photos, so we receive and store photos for those people. Some people enjoy watching videos on Facebook; when they do, we receive information about the video they watched, and we can use that information to help show other videos in their News Feeds. Other people seldom or never watch videos, so we do not receive the same kind of information from them, and their News Feeds are likely to feature fewer videos.

The data we have about people also depends on how they have used our controls. For example, people who share photos can easily delete those photos. The same is true of any other kind of content that people post on our services. Through Facebook's Activity Log tool, people can also control the information about their engagement—*i.e.,* their likes, shares and comments—with other people's posts. The use of these controls of course affects the data we have about people.

We recently announced improvements to our Download Your Information tool, as well as a new feature that makes it easier for people to see the information that's in their account on Facebook. These recently-expanded tools for accessing your information will allow people to see their data, delete it, and easily download and export it.

Question 3. Please list all data that Facebook generates based on user inputs.

Answer. Depending on which Services a person uses, we collect different kinds of information from or about them. This is described in our Data Policy:

- *Things you and others do and provide.* Information and content you provide. We collect the content, communications, and other information you provide when you use our Products, including when you sign up for an account, create or share content, and message or communicate with others. This can include information in or about the content you provide (like metadata), such as the location of a photo or the date a file was created. It can also include what you see through features we provide, such as our camera, so we can do things like suggest masks and filters that you might like, or give you tips on using camera formats. Our systems automatically process content and communications you and others provide to analyze context and what's in them for the purposes described below. Learn more about how you can control who can see the things you share.
  - Data with special protections. You can choose to provide information in your Facebook profile fields or Life Events about your religious views, political views, who you are "interested in," or your health. This and other information (such as racial or ethnic origin, philosophical beliefs, or trade union membership) could be subject to special protections under the laws of your country.
- *Networks and connections*. We collect information about the people, Pages, accounts, hashtags, and groups you are connected to and how you interact with them across our Products, such as people you communicate with the most or groups you are part of. We also collect contact information if you choose to upload, sync or import it from a device (such as an address book or call log or SMS log history), which we use for things like helping you and others find people you may know and for the other purposes listed below.
- *Your usage*. We collect information about how you use our Products, such as the types of content you view or engage with; the features you use; the actions you take; the people or accounts you interact with; and the time, frequency and duration of your activities. For example, we log when you're using and have last used our Products, and what posts, videos, and other content you view on our Products. We also collect information about how you use features like our camera.
- *Information about transactions made on our Products.* If you use our Products for purchases or other financial transactions (such as when you make a purchase in a game or make a donation), we collect information about the purchase or transaction. This includes payment information, such as your credit or debit card number and other card information; other account and authentication information; and billing, shipping and contact details.
- *Things others do and information they provide about you.* We also receive and analyze content, communications, and information that other people provide when they use our Products. This can include information about you, such as when others share or comment on a photo of you, send a message to you, or upload, sync or import your contact information.
- *Device Information.* As described below, we collect information from and about the computers, phones, connected TVs and other web-connected devices you use that integrate with our Products, and we combine this information across different devices you use. For example, we use information collected about your use of our Products on your phone to better personalize the content (including ads) or features you see when you use our Products on another device, such as your laptop or tablet, or to measure whether you took an action in response to an ad we showed you on your phone on a different device.

  Information we obtain from these devices includes:
  - Device attributes: information such as the operating system, hardware and software versions, battery level, signal strength, available storage space, browser type, app and file names and types, and plugins.
  - Device operations: information about operations and behaviors performed on the device, such as whether a window is foregrounded or backgrounded, or mouse movements (which can help distinguish humans from bots).
  - Identifiers: unique identifiers, device IDs, and other identifiers, such as from games, apps or accounts you use, and Family Device IDs (or other identifiers unique to Facebook Company Products associated with the same device or account).
  - Device signals: Bluetooth signals, and information about nearby Wi-Fi access points, beacons, and cell towers.

- Data from device settings: information you allow us to receive through device settings you turn on, such as access to your GPS location, camera, or photos.
- Network and connections: information such as the name of your mobile operator or ISP, language, time zone, mobile phone number, IP address, connection speed and, in some cases, information about other devices that are nearby or on your network, so we can do things like help you stream a video from your phone to your TV.
- Cookie data: data from cookies stored on your device, including cookie IDs and settings. Learn more about how we use cookies in the Facebook Cookies Policy and Instagram Cookies Policy.

- *Information from partners.* Advertisers, app developers, and publishers can send us information through Facebook Business Tools they use, including our social plug-ins (such as the Like button), Facebook Login, our APIs and SDKs, or the Facebook pixel. These partners provide information about your activities off Facebook—including information about your device, websites you visit, purchases you make, the ads you see, and how you use their services—whether or not you have a Facebook account or are logged into Facebook. For example, a game developer could use our API to tell us what games you play, or a business could tell us about a purchase you made in its store. We also receive information about your online and offline actions and purchases from third-party data providers who have the rights to provide us with your information. Partners receive your data when you visit or use their services or through third parties they work with. We require each of these partners to have lawful rights to collect, use and share your data before providing any data to us.

Application of European Data Protection Rules

Facebook is not the first company to experience a data breach or have its users' data misappropriated. Previously disclosed data breaches include Equifax, Uber, Yahoo, eBay, AOL, Target, and Home Depot. This suggests that there is a real need for a Federal regulatory scheme.

The European Union recently adopted the General Data Protect Regulation (GDPR), which requires businesses to protect the personal data and privacy of EU citizens. These EU rules also protect the exportation of personal data outside the EU.

On April 4, 2018, Mr. Zuckerberg publicly committed to "make all the same controls and settings available everywhere, not just in Europe."

However, according to an April 2018 Reuters report, Facebook intends on altering its terms of service to ensure that non-EU users will have their data processed by Facebook USA. The result is change is that GDPR protections would no longer cover the more than 1.5 billion international Facebook users who are not EU citizens.

Question 1. Is Facebook still committed to making GDPR privacy settings available to "everywhere"?

Answer. Yes. The controls and settings that Facebook is enabling as part of GDPR are available to people around the world, including settings for controlling our use of face recognition on Facebook and for controlling our ability to use data we collect off Facebook Company Products to target ads. We recently began providing direct notice of these controls and our updated terms to people around the world (including in the U.S.), allowing people to choose whether or not to enable or disable these settings or to consent to our updated terms. We provide the same tools for access, rectification, erasure, data portability, and others to people in the U.S. and rest of world that we provide in Europe, and many of those tools (like our Download Your Information tool, ad preferences tool, and Activity Log) have been available globally for many years.

a. For users in the United States, will Facebook commit to adopting a broad definition of "personal information" including information associated with an identifier number rather than a name is exempt from regulation?

Answer. Facebook is generally not opposed to regulation but wants to ensure it is the right regulation. The issues facing the industry are complex, multi-faceted, and affect an important part of peoples' lives. As such, Facebook is absolutely committed to working with regulators, like Congress, to craft the right regulations. Facebook would be happy to review any proposed legislation and provide comments.

b. For users in the United States, will Facebook commit to requiring affirmative consent should they seek to use or disclose personal information?

Answer. We are seeking explicit consent from people in Europe to three specific uses of data: facial recognition data (which previously was not enabled in Europe), special categories of data, and use of data we collect off Facebook Company Products to target ads. We recently began providing direct notice of these controls and our

updated terms to people around the world (including in the U.S.), allowing people to choose whether or not to enable or disable these settings or to agree to our updated terms. Outside of Europe we are not requiring people to complete those flows if they repeatedly indicate that they do not want to go through the experience. At the same time, the events of recent months have underscored how important it is to make sure people know how their information is used and what their choices are. So, we decided to communicate prominently on Facebook—through a full-screen message and a reminder to review at a later date. People can choose to dismiss or ignore these messages and continue using Facebook.

GDPR does not require consent for most uses of personal information, and instead, recognizes that many uses of data are necessary to provide a service or within a companies' legitimate interests or the public interest. We agree that different levels of consent or notice are appropriate depending on the type of information or contemplated use at issue.

c. For users in the United States, will Facebook allow customers to access, correct, retrieve, and delete their personal information?

Answer. We enable people, including people in the United States, to learn more about the data we collect through interactive tools such as Download Your Information, which lets people download a file containing data that they may want to take to another service, and through Access Your Information, a tool we've launched for people to more easily access and manage their data on Facebook. People can also control their information through their Settings and the Privacy Shortcuts tool that we're rolling out now.

d. For users in the United States, will Facebook commit to requiring individual notification in the event of a data breach?

Answer. Yes.

Question 2. If not, please explain why Facebook no longer will apply GDPR protections to all Facebook users.

Answer. As explained in the previous question, the controls and settings that Facebook is enabling as part of GDPR are already available to other people around the world, including settings for controlling our use of face recognition on Facebook and for controlling our ability to use data we collect off Facebook Company Products to target ads. We also provide the same tools for access, rectification, erasure, data portability, and others to people in the U.S. and rest of world that we provide in Europe, and many of those tools (like our Download Your Information tool, Ads Preferences tool, and Activity Log) have been available globally for many years.

Question 3. If Facebook does not intend to make GDPR protections available to users in the United States, please explain in detail how Facebook will ensure these users are covered by robust data protection policies?

Answer. As explained in the previous response, Facebook will be making the same controls and settings available under GDPR to people in the U.S.

Question 4. Will Facebook change its default settings to minimize the collection and use of U.S. user data?

Answer. We regularly review and update our settings to help people protect their privacy and give people choices about how their information is used and who can see it. That's why, for example, in 2014 we changed the default audience for posts from Public to Friends, and why we now ask people when they create a new account who they would like to see the things they post—their friends, the public, or a different audience.

Foreign Propaganda and Facebook Revenue

Last November, the Senate Intelligence Committee held a hearing on Social Media Influence in our 2016 elections where executives from Facebook, Twitter and Google testified. Following the hearing, I submitted 50 written questions to Facebook and the other companies.

The responses I received were evasive and some were nonresponsive. Please respond to the following question to the best of your ability. Where you have learned new information since submitting answers to previous QFRs, please supplement and amend your previous answers.

Question 1. How much revenue does Facebook earn from the user engagement that results from foreign propaganda?

Answer. We believe that annual revenue that is attributable to inauthentic or false accounts is immaterial.

Question 2. How much revenue does Facebook earn from the user engagement that results from fake news?

Answer. See Response to Question 1.

Question 3. How much revenue does Facebook earn from the user engagement that results from hyper-partisan content?

Answer. We do not have a definition of hyper-partisan, as defining what is hyper-partisan is difficult and controversial.

Question 4. What does Facebook do with money received from an entity that is found, either through internal audits or third-party notification, to be using the platform to distribute foreign propaganda, fake news, or hyper-partisan content?

Answer. Fraudulent ads are not allowed on Facebook. They are in breach of our advertising policies and we will remove them when we find them. Where we discover ads that violate our policies or applicable laws, we do not generally return money to those attempting to deceive our users. Instead, we make investments in areas to improve security on Facebook and beyond. In addition, the investments that we are making to address security issues are so significant that we have informed investors that we expect that the amount that we will spend will impact our profitability.

Question 5. How many employees are dedicated to addressing foreign propaganda?

Answer. We expect to have at least 250 people specifically dedicated to safeguarding election integrity on our platforms, and that number does not include the thousands of people who will contribute to this effort in some capacity. This type of abuse touches a number of different teams at Facebook. Thousands on our Business Integrity team will be working to better enforce our ad policies and to review more ads, and a significant number of engineers will build tools to identify ad and election abuse, and to enable us to follow through on our commitment to bring greater transparency to ads with political content.

Facebook Data Abuse Bounty

In April 2018, Facebook's announced a new "Data Abuse Bounty" program to "reward people who report any misuse of data by app developers."

According to your press release, "this program will reward people with first-hand knowledge and proof of cases where a Facebook platform app collects and transfers people's data to another party to be sold, stolen or used for scams or political influence."

Facebook also promised to shut down any offending apps if it confirms that an app has abused user data.

Question 1. Please list what abuses of data this program has identified and whether Facebook has investigated or is in the process of investigating these abuses.

Answer. This is a pilot program. We assess all submissions for validity, and if valid, conduct an investigation. Since launching the program we have received and are reviewing hundreds of reports. Updates about the Bug Bounty Program and the Data Abuse Bounty Program will be posted at *https://www.facebook.com/bugbounty* and *https://www.facebook.com/data-abuse*.

Question 2. Please list how many offending apps have been identified and subsequently shut down.

Answer. Since launching the program we have received and are reviewing hundreds of reports. Updates about the Bug Bounty Program and Data Abuse Bounty Program will be posted at *https://www.facebook.com/bugbounty* and *https://www.facebook.com/data-abuse*.

Question 3. Please explain how and when you intend to notify users impacted by newly-discovered data abuses.

Answer. Where we find evidence that these or other apps did misuse data, we will ban them and notify people whose data was shared with these apps.

Question 4. Upon identifying a malicious app, has Facebook considered other punitive measures beyond denying apps access to the platform (such as fines, lawsuits, etc.)? If not, please explain why not.

Answer. We use a variety of tools to enforce Facebook policies against violating parties, including developers. We review tens of thousands of apps per year and regularly disapprove noncompliant apps as part of our proactive review process. We also use tools like cease and desist letters, account suspensions, letter agreements, and civil litigation. For example, since 2006, Facebook has sent over 1,150 cease-and-desist letters to over 1,600 targets. In 2017, we took action against about 370,000 apps, ranging from imposing certain restrictions to removal of the app from the platform. Moreover, we have required parties who have procured our data without authorization to delete that data. We have invested significant resources in these efforts. Facebook is presently investigating apps that had access to large amounts of information before we changed our platform policies in 2014 to significantly reduce the data apps could access. To date around 200 apps (from a handful of developers: Kogan, AIQ, Cube You, the Cambridge Psychometrics Center,

myPersonality, and AIQ) have been suspended—pending a thorough investigation into whether they did in fact misuse any data.

Additionally, we have suspended an additional 14 apps, which were installed by around one thousand people. They were all created after 2014, after we made changes to more tightly restrict our platform APIs to prevent abuse. However, these apps appear to be linked to AIQ, which was affiliated with Cambridge Analytica.

Embedding Employees in Campaigns

Facebook often embeds staff with advertising clients to help them target their campaigns. Brad Parscale, the Trump Campaign's digital director, said of Facebook: "we had their staff embedded inside our offices," and "Facebook employees would show up for work every day in our offices." Mr. Parscale said that staff provided to the Trump Campaign by Facebook and other companies worked "side by side" with Cambridge Analytica.

Press reports indicate that Cambridge Analytica ultimately had 13 people working on the Trump campaign's digital operation, headquartered in San Antonio.

Question 1. What services did embedded Facebook staff provide?

Answer. Facebook representatives advise political advertisers on Facebook, as they would with other, non-political managed accounts. During the 2016 election cycle, Facebook worked with campaigns to optimize their use of the platform, including helping them understand various ad formats and providing other best practices guidance on use of the platform. No one from Facebook was assigned full-time to the Trump campaign, or full-time to the Clinton campaign.

Question 2. Did these employees have a set of rules, standards or regulations under which they provide these services?

Answer. We have a compliance team that trains our sales representatives to comply with all Federal election law requirements in this area.

Question 3. Was there a mechanism through which they could alert Facebook if they had concerns about the campaign's activities?

Answer. Facebook employees are encouraged to raise any concerns about improper activity to their managers.

Question 4. How many people did Facebook send to San Antonio to work with the Trump Campaign's digital operation? For how long?

Answer. We offered identical support to both the Trump and Clinton campaigns, and had teams assigned to both. Everyone had access to the same tools, which are the same tools that every campaign is offered. The campaigns did not get to "hand pick" the people who worked with them from Facebook. And no one from Facebook was assigned full-time to the Trump campaign, or full-time to the Clinton campaign. Both campaigns approached things differently and used different amounts of support.

Question 5. Did Facebook employees embedded with the campaign work directly or indirectly with Cambridge Analytica?

Answer. While no one from Facebook was assigned full-time to the Trump campaign, Facebook employees did interact with Cambridge Analytica employees. While our investigation is ongoing, our review indicates that Facebook employees did not identify any issues involving the improper use of Facebook data in the course of their interactions with Cambridge Analytica during the 2016 U.S. Presidential campaign.

Question 6. What, exactly, did the Facebook "embeds" work on with Cambridge Analytica in San Antonio?

Answer. In general, political data firms working on the 2016 campaign had access to Facebook's advertising support services, including technical support, and best practices guidance on how to optimize their use of Facebook. Everyone had access to the same tools, which are the same tools that every campaign is offered. No one from Facebook was assigned full-time to the Trump campaign.

Question 7. Were Facebook employees aware of data sets that may have been scraped from Facebook users?

Answer. While our investigation is ongoing, our review indicates that Facebook employees did not identify any issues involving the improper use of Facebook data in the course of their interactions with Cambridge Analytica during the 2016 U.S. Presidential campaign.

Question 8. Did Facebook work with Cambridge Analytica, directly or indirectly, on ad optimization or voter targeting?

Answer. Facebook representatives provide general ad support to political advertisers on Facebook, as they do with other, non-political managed accounts. During the 2016 election cycle, for example, Facebook provided technical support and best

practices guidance to advertisers, including Cambridge Analytica, on using Facebook's advertising tools.

Question 9. Did Cambridge Analytica or Parscale's digital operation purchase media on Facebook?

Answer. Yes.

Question 10. Reports suggest that the Special Counsel has met with at least one Facebook employee who worked in San Antonio. Is Facebook cooperating fully with the investigation?

Answer. We have stated publicly that we have cooperated with the Special Counsel.

Question 11. What role has Facebook played in supporting Cambridge Analytica/SCL work on elections in other countries (in Africa, the Caribbean, former Soviet Republics, etc.)?

Answer. Facebook did not provide support to Cambridge Analytica/SCL in connection with elections in other countries. It also appears from the best information we have to date that Kogan only provided SCL with data on Facebook users from the United States. Kogan and SCL have consistently maintained that Kogan never provided SCL with any data for Facebook users outside the United States, which is supported by a contract between Kogan's company and SCL, which was furnished by Christopher Wylie to the UK Parliament.

Question 12. Did Facebook, in the past 4 years, embed employees with Cambridge Analytica for foreign electoral campaigns/referenda, including Brexit or elections in Nigeria, Kenya, the Czech Republic, Lithuania, or Georgia?

Answer. No.

Question 13. Has Facebook ever provided support to Secure America Now, a political action committee targeting swing state voters with anti-Muslim messaging?

Answer. We did not work directly with Secure America Now; we worked through a third-party advertising agency. Neither did we create any content for Secure America Now. As is customary across managed advertising agencies, we provided a general best practices training to the agency staff. As is also customary, we provided the measurement tools to determine the efficacy of the ads and differences between formats.

Question 14. Who at Facebook would have overseen work on this account?

Answer. We did not work directly with Secure America Now; we worked through a third-party advertising agency.

Question 15. Did it raise any ethical concerns within Facebook? If not, please explain.

Answer. See Response to Question 13.

We recognize how important it is for Facebook to be a place where people feel empowered to communicate, and we take our role in keeping abuse off our service seriously. Our mission entails embracing diverse views. We err on the side of allowing content, even when some find it objectionable, unless removing that content prevents a specific harm. That said, we do not allow hate speech on our platform because it creates an environment of intimidation and exclusion and in some cases may promote real-world violence.

We define hate speech as a direct attack on people based on what we call protected characteristics—race, ethnicity, national origin, religious affiliation, sexual orientation, sex, gender, gender identity, and serious disability or disease. We also provide some protections for immigration status. We define attack as violent or dehumanizing speech, statements of inferiority, and calls for exclusion or segregation. Our detailed hate speech policies are available at *https://www.facebook.com/communitystandards/objectionable_content/hate_speech*.

We have Community Standards that prohibit hate speech, bullying, intimidation, and other kinds of harmful behavior. We hold advertisers to even stricter advertising policies to protect you from things like discriminatory ads—and we have recently tightened our ad policies even further to prohibit additional shocking and sensational content.

Third-Party Data Aggregators and Third-Party Transfers

Prior to March 2017, Facebook worked with third-party data aggregators to enhance existing data sets. As a result, advertisers had access to data collected by Facebook and data collected by third parties such as Experian and Acxion.

In the aftermath of the Facebook-Cambridge Analytica debacle, Facebook announced that it would be shutting down Partner Categories and that third-party data providers would no longer be able to offer their targeting directly on Facebook.

This verbal commitment is laudable but must be implemented in order to ensure the public's data are safeguarded.

Question 1. Please detail any efforts Facebook has initiated and/or completed to identify other improper third-party data transfers.

Answer. We are in the process of investigating every app that had access to a large amount of information before we changed our Platform in 2014. If we find suspicious activity, we will take immediate steps to investigate (including a full forensic audit) or take enforcement actions against the app. If we determine that there has been improper use of data, we will ban those developers and notify everyone affected. Facebook is launching the Data Abuse Bounty to reward people who report any misuse of data by app developers. The Data Abuse Bounty, inspired by the existing bug bounty program that we use to uncover and address security issues, will help us identify violations of our policies.

Question 2. What, if any, external audits has Facebook completed to ensure that all third parties are following Facebook privacy policies?

Answer. See Response to Question 1.

Facebook's New Partnership with Independent Researchers

On April 9, 2018 the William and Flora Hewlett Foundation, announced it would fund a research initiative to examine Facebook's role in elections and democracy.

The fund will support an independent committee of scholars who will define research topics and vet research proposals that explore the intersection of elections, democracy, and social media.

In addition, according to media reports, Facebook has reportedly agreed to give research accesses to proprietary data.

Question 1. Facebook has limited this new initiative to prospective studies. Will Facebook commit to allowing studies of Russian interference in the 2016 election?

Answer. Facebook recently announced a new initiative to help provide independent, credible research about the role of social media in elections, as well as democracy more generally. It will be funded by the Laura and John Arnold Foundation, Democracy Fund, the William and Flora Hewlett Foundation, the John S. and James L. Knight Foundation, the Charles Koch Foundation, the Omidyar Network, and the Alfred P. Sloan Foundation. At the heart of this initiative will be a group of scholars who will:

- Define the research agenda;
- Solicit proposals for independent research on a range of different topics; and
- Manage a peer review process to select scholars who will receive funding for their research, as well as access to privacy-protected datasets from Facebook which they can analyze.

Facebook will not have any right to review or approve their research findings prior to publication. More information regarding the study is available at *https://newsroom.fb.com/news/2018/04/new-elections-initiative/*.

Question 2. The new initiative also does not appear to cover studies on privacy and security, even though those are some of the most pressing issues related to your platform. Will you commit to expanding the initiative to cover privacy and security?

Answer. We regularly work with privacy experts outside the company, including academics, to understand how to improve privacy protections for people on Facebook and to support efforts to improve privacy protections for people overall. For example, we recently hosted a workshop for privacy academics to discuss research around online privacy and worked with academics as a part of recent privacy consultations that we have conducted at our headquarters and around the world.

Also, we recently announced plans to collaborate with academics and other privacy experts as a part of our efforts to build Clear History, a new feature that will enable people to see the websites and apps that send us information when they use them, delete this information from their account, and turn off our ability to store it associated with their account going forward.

Question 3. Given that many of the issues with Facebook relate to income, ethnicity, gender, sexual orientation, and other diverse groups, will you commit to ensuring that this committee includes individuals who will adequately represent perspectives of these diverse groups?

Answer. In consultation with the foundations funding the initiative, Facebook will invite respected academic experts to form a commission which will then develop a research agenda about the impact of social media on society—starting with elections. We are keen to have a broad range of experts—with different political outlooks, expertise and life experiences, gender, ethnicity, and from a broad range of countries.

Discriminatory Ad Practices

Facebook offers advertisers "targeting categories" that range from ethnic affinity, education level, political affiliation, and employment status. The categories may seem innocuous but invariably serve as proxies for demographic characteristics such as race, family status, class, and sexual orientation.

A recent *Pro Publica* report revealed that, in February 2017, companies could still buy rental-housing ads on Facebook and request that those ads not be shown to certain categories of users including African Americans, mothers of high school kids, people interested in wheelchair ramps, Jewish people, and Spanish speakers.

As of March 27, 2018 housing rights advocates are suing Facebook in Federal court for allowing real estate brokers and landlords to exclude select certain categories—family status, sex, and disability—when targeting advertisements.

Question 1. Does Facebook still allow advertisers to target based on the abovementioned categories?

Answer. Discriminatory advertising has no place on Facebook's platform and Facebook removes such content as soon as it becomes aware of it. Facebook's policies prohibit advertisers from discriminating against people on personal attributes such as race, ethnicity, color, national origin, religion, age, sex, sexual orientation, gender identity, family status, disability, and medical or genetic conditions. Facebook educates advertisers on our anti-discrimination policy, and in some cases, requires the advertisers to certify compliance with Facebook's anti-discrimination policy and anti-discrimination laws.

Facebook also uses machine learning to help identify ads that offer housing, employment, or credit opportunities. When an advertiser attempts to show an ad that Facebook identifies as offering a housing, employment, or credit opportunity and includes Facebook's multicultural advertising segments, Facebook will disapprove the ad. Facebook also requires advertisers to certify that they are complying with Facebook's updated anti-discrimination policy and anti-discrimination laws when the advertiser attempts to show a housing, employment, or credit opportunity and uses any other audience segment on Facebook.

Question 2. Do you agree this categorization lends itself to discriminatory practices?

Answer. See Response to Question 1.

Question 3. As Facebook works to reform company policies, how will Facebook protect the civil rights of all Facebook users?

Answer. We have Community Standards that prohibit hate speech, bullying, intimidation, and other kinds of harmful behavior. We hold advertisers to even stricter advertising policies to protect users from things like discriminatory ads. We don't want advertising to be used for hate or discrimination, and our policies reflect that. For example, we make it clear that advertisers may not discriminate against people based on personal attributes such as race, ethnicity, color, national origin, religion, age, sex, sexual orientation, gender identity, family status, disability, and medical or genetic condition. We educate advertisers on our anti-discrimination policy, and in some cases—including when we detect that an advertiser is running a housing ad—we require advertisers to certify compliance with our anti-discrimination policy and anti-discrimination laws.

We look forward to finding additional ways to combat discrimination, while increasing opportunity for underserved communities, and to continuing our dialogue with policymakers and civil rights leaders about these important issues.

Question 4. Will you commit to modifying your existing policies and procedures to ensure that housing discrimination is prohibited on your platform?

Answer. See Response to Question 3.

2015 Cambridge Analytical Leak and Decision not to Notify Users

On March 17, 2018, the *New York Times* reported that the data analytics firm, Cambridge Analytica, had secretly harvested the personal data of millions of Facebook users.

Reports have confirmed that Facebook knew of this data breach in December 2015, but declined to notify the affected users.

On April 10, 2018, Mr. Zuckerberg confirmed that such a decision had, in fact, been made. At a Joint hearing with the Senate Commerce and Judiciary Committees, when asked whether there was "decision made [by Facebook] not to inform the users [of the breach]," Mr. Zuckerberg replied "that is my understanding, yes."

Question 1. Please explain how, and when, Facebook first became aware of Cambridge Analytica's misappropriation of Facebook users' data?

Answer. On December 11, 2015, *The Guardian* published an article reporting that Kogan and his company, GSR, may have passed information the app had obtained

from Facebook users to SCL Elections Ltd. (SCL)/Cambridge Analytica. As part of its investigation, Facebook contacted Kogan and Cambridge Analytica to investigate the allegations reflected in the reporting. Thereafter, Facebook obtained written certifications or confirmations from Kogan, GSR, and other third parties (including Cambridge Analytica and SCL) declaring that all such data they had obtained was accounted for and destroyed. In March 2018, Facebook received information from the media suggesting that the certification we received from SCL may not have been accurate and immediately banned SCL Group and Cambridge Analytica from purchasing advertising on our platform. Since then, Facebook has been actively investigating the issue, including pursuing a forensic audit of Cambridge Analytica, which is currently paused at the request of the UK Information Commissioner's Office (which is separately investigating Cambridge Analytica).

Mr. Zuckerberg did not become aware of allegations that Cambridge Analytica may not have deleted data about Facebook users obtained from Kogan's app until March of 2018, when these issues were raised in the media.

Question 2. What steps did Facebook take in deciding not to inform impacted Facebook users of Cambridge Analytica's misappropriation of their data? When did Facebook decide not to inform Facebook users who were impacted?

Answer. When Facebook learned about Kogan's breach of Facebook's data use policies in December 2015, it took immediate action. The company retained an outside firm to assist in investigating Kogan's actions, to demand that Kogan and each party he had shared data with delete the data and any derivatives of the data, and to obtain certifications that they had done so. Because Kogan's app could no longer collect most categories of data due to changes in Facebook's platform, the company's highest priority at that time was ensuring deletion of the data that Kogan may have accessed before these changes took place. With the benefit of hindsight, we wish we had notified people whose information may have been impacted. Facebook has since notified all people potentially impacted with a detailed notice at the top of their newsfeed.

Question 3. Who at Facebook made the decision not to inform Facebook users?

Answer. See Response to Question 2.

Question 4. What was the rationale for this decision?

Answer. See Response to Question 2.

Question 5. When did Mr. Zuckerberg learn of this breach and the decision not to inform users?

Answer. See Response to Question 2.

Question 6. Are there changes in place to improve the way Facebook responds to these breaches in the future?

Answer. Facebook allows people to view, manage, and remove the apps that they have logged into with Facebook through the App Dashboard. We recently prompted everyone to review their App Dashboard as a part of a Privacy Checkup, and we also provided an educational notice on Facebook to encourage people to review their settings. More information about how users can manage their app settings is available at *https://www.facebook.com/help/218345114850283?helpref=about_content*.

The categories of information that an app can access is clearly disclosed before the user consents to use an app on Facebook platform. Users can view and edit the categories of information that apps they have used have access to through the App Dashboard.

Question 7. Please list other instances of abuse where Facebook user data was misappropriated and a decision was made not to inform users or where the company failed to inform users.

Answer. See Response to Question 6.

Annual Transparency Report

On June 1, 2017 Facebook shareholders voted down a transparency proposal requesting that "Facebook issue a report reviewing the public policy issues associated with fake news enabled by Facebook. The report should review the impact of current fake news flows and management systems on the democratic process, free speech, and a cohesive society, as well as reputational and operational risks from potential public policy developments."

Facebook's board of directors urged a no vote on the proposal, calling the report "unnecessary" and "not beneficial to shareholders." The shareholder proposal failed.

Since then, Facebook has publicly acknowledged that Russian actors purchased ads to manipulate and interfere with the election. It took Facebook two years and a whistleblower before to disclose the data breach by Cambridge Analytica.

It appears that the ordinary practice and tendency of Facebook—like most other companies—is to advocate for less disclosure.

Question 1. Will Facebook commit to producing an annual public transparency report to your shareholders?

Answer. Facebook publishes an annual transparency report, the most recent report was issued on May 15, 2018 and can be found here: *https://transparency.facebook.com/*.

○