FACIAL RECOGNITION TECHNOLOGY: PART I ITS IMPACT ON OUR CIVIL RIGHTS AND LIBERTIES

HEARING

BEFORE THE

COMMITTEE ON OVERSIGHT AND REFORM HOUSE OF REPRESENTATIVES

ONE HUNDRED SIXTEENTH CONGRESS

FIRST SESSION

MAY 22, 2019

Serial No. 116–27

Printed for the use of the Committee on Oversight and Reform

Available on: *http://www.govinfo.gov*
http://www.oversight.house.gov
http://www.docs.house.gov

U.S. GOVERNMENT PUBLISHING OFFICE

36–663 PDF WASHINGTON : 2019

COMMITTEE ON OVERSIGHT AND REFORM

ELIJAH E. CUMMINGS, Maryland, *Chairman*

CAROLYN B. MALONEY, New York
ELEANOR HOLMES NORTON, District of Columbia
WM. LACY CLAY, Missouri
STEPHEN F. LYNCH, Massachusetts
JIM COOPER, Tennessee
GERALD E. CONNOLLY, Virginia
RAJA KRISHNAMOORTHI, Illinois
JAMIE RASKIN, Maryland
HARLEY ROUDA, California
KATIE HILL, California
DEBBIE WASSERMAN SCHULTZ, Florida
JOHN P. SARBANES, Maryland
PETER WELCH, Vermont
JACKIE SPEIER, California
ROBIN L. KELLY, Illinois
MARK DESAULNIER, California
BRENDA L. LAWRENCE, Michigan
STACEY E. PLASKETT, Virgin Islands
RO KHANNA, California
JIMMY GOMEZ, California
ALEXANDRIA OCASIO-CORTEZ, New York
AYANNA PRESSLEY, Massachusetts
RASHIDA TLAIB, Michigan

JIM JORDAN, Ohio, *Ranking Minority Member*
JUSTIN AMASH, Michigan
PAUL A. GOSAR, Arizona
VIRGINIA FOXX, North Carolina
THOMAS MASSIE, Kentucky
MARK MEADOWS, North Carolina
JODY B. HICE, Georgia
GLENN GROTHMAN, Wisconsin
JAMES COMER, Kentucky
MICHAEL CLOUD, Texas
BOB GIBBS, Ohio
RALPH NORMAN, South Carolina
CLAY HIGGINS, Louisiana
CHIP ROY, Texas
CAROL D. MILLER, West Virginia
MARK E. GREEN, Tennessee
KELLY ARMSTRONG, North Dakota
W. GREGORY STEUBE, Florida

DAVID RAPALLO, *Staff Director*
YVETTE BADU-NIMAKO, *Legislative Director/Counsel*
GINA KIM, *Counsel*
LAURA RUSH, *Deputy Chief Clerk/Security Manager*
CHRISTOPHER HIXON, *Minority Staff Director*
CONTACT NUMBER: 202-225-5051

C O N T E N T S

INDEX OF DOCUMENTS

The documents entered into the record during this hearing are listed below, and are available at: https://docs.house.gov.

FACIAL RECOGNITION TECHNOLOGY: PART I ITS IMPACT ON OUR CIVIL RIGHTS AND LIBERTIES

Wednesday, May 22, 2019

HOUSE OF REPRESENTATIVES
COMMITTEE ON OVERSIGHT AND REFORM
WASHINGTON, D.C.

The committee met, pursuant to notice, at 10:27 a.m., in room 2154, Rayburn Office Building, Hon. Elijah E. Cummings, (chairman of the committee) presiding.

Present: Representatives Cummings, Maloney, Norton, Clay, Lynch, Connolly, Krishnamoorthi, Raskin, Rouda, Hill, Welch, Kelly, DeSaulnier, Plaskett, Khanna, Gomez, Ocasio-Cortez, Pressley, Tlaib, Jordan, Amash, Massie, Meadows, Grothman, Comer, Cloud, Gibbs, Higgins, Miller, Green, and Steube.

Chairman CUMMINGS. The committee will come to order.

Without objection, the chair is authorized to declare a recess of the committee at any time. I now recognize myself for five minutes for an opening statement.

Today, we are having our first hearing of this Congress on the use of facial recognition technology. The Oversight Committee is uniquely suited to conduct a comprehensive review of this issue because we have extremely wide-ranging jurisdiction.

We can look across all Federal agencies, state and local entities, and the private sector as well. I want to make clear at the onset that this is a bipartisan issue.

Both the conservatives and liberals alike have real questions about when they are being monitored, why they are being monitored, who is monitoring them, and what happens to this information after it is collected.

We have been working closely with the ranking member, Mr. Jordan, and I sincerely appreciate his advice and his assistance and the assistance of his staff in bringing this hearing together.

Facial recognition is a fascinating technology with huge potential to effect a number of different applications. But right now it is virtually unregulated.

In 2016, the Government Accountability Office issued a report recommending that the FBI make numerous changes to its facial recognition data base to improve data security and ensure accuracy, privacy, and transparency.

However, just last month GAO sent a letter highlighting six priority recommendations that the FBI has yet to fully implement. At the local levels, cities like Detroit and Chicago are rapidly expand-

ing the use of facial recognition technology to track its citizens in real time.

At the same time, other cities, like San Francisco, are going in completely the opposite direction, banning the government use of facial technology all together.

Of course, we all see how private companies are using this technology more and more for advertisements, security, and a variety of different customer experiences.

But again, there are virtually no controls on where this information goes. In 2017, our committee held a hearing to review the law enforcement use of facial recognition technology. As part of that hearing we found that 18 states have memoranda of understanding with the FBI to share their data bases.

As a result, more than half of American adults are part of facial recognition data bases and they may not even know it. We also heard testimony that facial recognition technology misidentifies women and minorities at a much higher rate than white males, increasing the risk of racial and gender bias.

This issue is very personal for me. My district includes Baltimore, where I have lived now my entire life. After the tragic death of Freddie Gray at the hands of the police in 2015, my city took to the streets in anger, frustration, and grief.

During that time, I also walked the streets of Baltimore along with religious leaders and people from our community. We walked together for two reasons: one, to protest this tremendous loss of life and, two, to urge our fellow citizens to find a peaceful resolution to this crisis.

Later we learned that the police used facial recognition technology to find and arrest protestors. It is likely that I and other members of our community who were simply exercising our rights under the Constitution were scanned, identified, and monitored by using this technology.

Think about what I just said. Whatever walk of life you may come from, you may very well be a part of this process. You could be at a rally supporting gun rights or protesting gun violence. You could be marching for the right to life or a woman's right to choose. You could be pressing for the repeal of the ACA or the expansion of health care.

In all of these cases the government can monitor you without your knowledge and enter your face into a data base that could be used in virtually unrestricted ways.

We need to do more to safeguard the rights of free speech and assembly under the First Amendment, the right to privacy under the Fourth Amendment, and the right of equal protection under the law under the Fourteenth Amendment.

My hope is that today's hearing can be a broad review of these issues, and we are honored and thankful to have such a distinguished panel as we have today.

On June 4, we will be having our second hearing on this topic and we will hear from law enforcement witnesses. After that I will be asking our subcommittees to conduct deeper dives on specific issues related to Federal law enforcement, state and local issues, and the private sector.

Our goal with this review is to identify sensible and concrete recommendations, legislative or otherwise, that recognize the benefits of this technology to protect against this abuse.

With that, I turn to our distinguished ranking member, Mr. Jordan, for his opening statement.

Mr. JORDAN. Mr. Chairman, thank you.

This is a critical hearing on a critical issue. Congressional oversight on this issue, I think, is of paramount importance and I do want to thank you because this committee has a history of working in a bipartisan manner when it comes to civil liberties, when it comes to privacy rights, and you have been a champion on that and I applaud your efforts and I am glad that we have got this nice panel to have a good discussion this morning.

A few years ago, we had a hearing on Stingray technology. I think some of you were at that hearing, if I remember correctly. But this is a technology where you have this device and instead of people's cell phones going to the tower it actually bounces off this device and folks' government can get your cell number and, frankly, know exactly where you are standing.

And as the chairman mentioned, the potential for mischief when you think about folks exercising their First Amendment liberties at some kind of political rally, whether it is on the right or the left, as the chairman talked about, I think is scary.

We learned in that hearing also that the IRS was actually involved in using this technology—the same IRS that a few years ago targeted people for their political beliefs. We found that—we found that very scary.

Stop and think then, not just the cell phone now but actually facial recognition in real-time video, as the chairman talked about, that is a scary thought. That is 1984 George Orwell kind of scenario that I think troubles us all.

So I am—I appreciate this hearing. I am glad that we are going to hear from our witnesses and get a chance to talk about this important subject and how, as the chairman said, it is virtually unregulated. But I think that, frankly, needs to change.

And so with that, Mr. Chairman, I would yield back and I look forward to hearing from our witnesses in the discussion that will ensue.

Chairman CUMMINGS. Now I—thank you very much.

Now I want to welcome our witnesses. Ms. Joy Buolamwini—thank you—founder of the Algorithmic Justice League, and Mr. Andrew Ferguson, professor of law, University of the District of Columbia, David A. Clarke School of Law, Ms. Clare Garvie, senior associate, Center on Privacy and Technology, Georgetown University Law Center, and Ms. Neema Singh Guliani——

Ms. GULIANI. Guliani.

Chairman CUMMINGS. No, you go ahead and say it.

Ms. GULIANI. Guliani.

Chairman CUMMINGS. I did the best I could with what I had.

Ms. GULIANI. You did good.

Chairman CUMMINGS. Thank you very much.

Who is a senior legislative counsel to the American Civil Liberties Union, and Dr. Cedric Alexander, former president, the National Organization of Black Law Enforcement Executives.

If you all would please stand and raise your right hand and I will now swear you in.

[Witness were sworn.]

Chairman CUMMINGS. Let the record show that the witnesses answered in the affirmative. Thank you, and please be seated.

I remind you that the microphones are extremely sensitive so please speak directly into them. Make sure it is on when you speak.

So without objection, your written Statements will be made part of the record. With that, Ms. Buolamwini, you are now recognized to give an oral presentation of your testimony.

STATEMENT OF JOY BUOLAMWINI, FOUNDER, ALGORITHMIC JUSTICE LEAGUE

Ms. BUOLAMWINI. Thank you.

Chairman Cummings, Ranking Member Jordan, and fellow committee members for the opportunity to testify. I am an algorithmic bias researcher based at MIT and I have conducted studies that show some of the largest recorded racial and skin type biases in AI systems sold by companies like IBM, Microsoft, and Amazon.

You have already heard facial recognition and related technologies have some flaws. In one test I ran Amazon recognition even failed on the face of Oprah Winfrey, labeling her male.

Personally, I have had to resort to literally wearing a white mask to have my face detected by some of this technology. Coding in white face is the last thing I expected to be doing at MIT, an American epicenter of innovation.

Now, given the use of this technology for mass surveillance, not having my face detected could be seen as a benefit. But besides being employed for dispensing toilet paper, in China the technology is being used to track Uighur Muslim minorities.

Beyond being abused, there are many ways for this technology to fail. Among the most pressing are misidentifications that can lead to false arrest and accusations.

Just last month in Rhode Island, a Brown University senior preparing for finals was misidentified as a terror suspect in the Sri Lanka Easter bombings.

The police eventually corrected the mistake but the damage was done. She received death threats and her family was put at risk. Mistaken identity is more than an inconvenience and can lead to grave consequences.

At a minimum, Congress should pass a moratorium on the police use of facial recognition as the capacity for abuse, lack of oversight, and technical immaturity poses too great a risk, especially for marginalized communities.

The Brown University senior, like me, is a woman of color under the age of 30. We fall into multiple groups that the technology repeatedly fails on the most, namely, people with nonwhite skin, women, and youth.

Due to the consequences of failures of this technology, I decided to focus my MIT research on the accuracy of facial analysis systems.

These studies found that for the task of guessing a gender of a face, IBM, Microsoft, and Amazon had errors of no more than 1 percent for lighter-skinned men.

In the worst case, those errors rose to over 30 percent for darker-skinned women. Given such accuracy disparities, I wondered how large tech companies could have missed these issues.

It boiled down to problematic data set choices. In evaluating benchmark data sets from organizations like NIST, the National Institute for Standards and Technology, I found some surprising imbalances.

One NIST data set was 75 percent male and 80 percent lighter skin, or what I like to call a pale male data set.

We cannot adequately evaluate facial analysis technologies without addressing this critical issue. Moving forward, the demographic and phenotypic composition of NIST benchmarks must be made public and updated to better inform decisionmakers about the maturity of facial analysis technology.

The harvesting of face data also requires guidelines and oversight. Companies like Facebook have built facial recognition capabilities by training their systems using our face data without expressed consent. But regulations make a difference.

As a result of GDPR, instead of the default, Facebook now makes facial recognition an opt-in feature for users in Europe. Americans should have the same assurances that they will not be subjected to Facebook facial recognition without consent.

No one should be forced to submit their face data to access widely used platforms, economic opportunity, or basic services. Just this week, a man sued Uber after having his driver's account deactivated due to facial recognition failures.

Tenants in Brooklyn are protesting the installation of an unnecessary face recognition entry system. New research is showing bias in the use of facial analysis technology for health care purposes and facial recognition is being sold to schools, subjecting children to face surveillance.

Our faces may well be the final frontier of privacy. Congress must act now to uphold American freedoms and rights. At a minimum, Congress should require all Federal agencies and organizations using Federal funding to disclose current use of face-based technologies. We cannot afford to operate in the dark.

Thank you for the invitation to testify and I welcome your questions.

Chairman CUMMINGS. Thank you very much.

Mr. Ferguson?

STATEMENT OF ANDREW G. FERGUSON, PROFESSOR OF LAW, UNIVERSITY OF THE DISTRICT OF COLUMBIA, DAVID A. CLARKE SCHOOL OF LAW;

Mr. FERGUSON. Chairman Cummings, Ranking Member Jordan, and members of the committee, thank you for the opportunity to testify today.

I am a law professor who studies the intersection of big data policing and Fourth Amendment freedoms. For the past decade, I have been studying how new surveillance technologies shape con-

stitutional rights and police powers, and based on that work, I have a very simple message for you today.

Congress must act—must act now to regulate facial recognition technologies because the case by case slow process of Fourth Amendment litigation is inadequate to address the rapidly changing world of mass surveillance.

I have five main points.

First, the Fourth Amendment will not save us from the privacy threat posed by facial recognition technology. The Supreme Court is making solid strides in trying to update Fourth Amendment principles in the face of these new technologies.

But they are chasing an accelerating train and will not catch up. Only legislation can respond to the real-time threats of real-time technology.

Second, the Fourth Amendment was never meant to be the sole source of government regulation. Instead, our entire constitutional system is premised upon Congress taking a leading role guided by and only in a rare instance overruled by our founding Constitution.

Indeed, one Supreme Court justice in particular—Justice Samuel Alito—has explicitly and repeatedly welcomed congressional assistance in this area.

In Riley v. California, Justice Alito said it would be very unfortunate if privacy protection in the 21st century were left primarily to the Federal courts using the blunt instrument of the Fourth Amendment.

Third, the few steps the Supreme Court has made on the subject of locational tracking technologies offer guidance about how to avoid drafting a law that could get struck down on Fourth Amendment grounds.

Just last year, the Supreme Court struck down provisions of the Stored Communications Act in Carpenter v. United States involving law enforcement acquisition of third party cell site records.

Such acquisition, held the court, typically requires a probable cause warrant. So as Congress debates creating standards to regulate facial recognition technology, this Fourth Amendment floor should be a baseline consideration.

Fourth, as Congress builds the scaffolding off that constitutional floor, we need to think about the technology not just through the lens of today but with an eye toward the expansion of surveillance technologies that will combine, aggregate, link, and share data in ways that will reshape the existing power dynamics of government and the people.

We are not just talking about technological hardware—cameras, computers, and tools—but systems of surveillance, in particular, Big Data policing systems that can process, store, and retrieve information in ways that has never been possible in past eras.

Legislation must future approve privacy protections with an eye toward the growing scope, scale, and sophistication of these systems of surveillance.

Finally, these Fourth Amendment questions must be coupled with a focus on First Amendment freedoms, civil rights, and fundamental fairness when it comes to public safety protections.

The burden of surveillance technology has never been equally shared across socioeconomic or racial groups. Surveillance is both

a civil rights issue and a civil liberties issue, and Congress needs to regulate with racial justice in mind.

In my written testimony, I have carefully laid out the different types of facial recognition that Congress needs to address today. Generalized face surveillance, monitoring without any individualized suspicion, investigative face recognition targeted with individualized suspicion, and separately non-law enforcement or emergency uses.

I have also attempted to analyze the Fourth Amendment implication to both face surveillance and face recognition with the conclusion, again, that the Fourth Amendment will not save us.

It will not satisfactorily resolve the core privacy questions. I would like to emphasize two points here which arise from my rather lengthy constitutional and legal analysis.

First, Federal legislation should be drafted to ban generalized face surveillance for all ordinary law enforcement purposes. Whether stored, real-time, or through third party image searches, building a system with a potential to arbitrarily scan and identify individuals without any criminal suspicion and to discover personal information about their location, interests, or activities can and should simply be banned by law.

Second, Federal legislation should authorize use of face recognition for investigative targeting only on a probable cause plus standard, requiring an assertion of probable cause and a sworn affidavit, plus declarations that care was taken to minimize the unintended collection of other face images and that proper steps have been taken to document and memorialize the collection.

This standard would apply to all face recognition including stored surveillance scans, real-time scans, third party image scans, and even government-collected image scans.

In my written testimony, I try to defend these recommendations as a matter of constitutional law and technological reality, and hope they offer a way forward—a bipartisan way forward—with specific legislative recommendations.

Last point. Unregulated facial recognition technology should not be allowed to continue. It is too powerful, too chilling, too undermining to principles of privacy, liberty, and security.

I am happy to answer any questions.

Chairman CUMMINGS. Thank you very much.

Ms. Garvie?

STATEMENT OF CLARE GARVIE, SENIOR ASSOCIATE, GEORGETOWN UNIVERSITY LAW CENTER, CENTER ON PRIVACY & TECHNOLOGY

Ms. GARVIE. Good morning, Chairman Cummings, Ranking Member Jordan, and distinguished members of the committee. Thank you for inviting me to speak to you today.

Face recognition presents unique threats to our civil rights and liberties. I would like to raise three core points about face recognition and our constitution that I hope will be helpful as this committee continues to examine this powerful technology.

First, face recognition gives law enforcement a power that they have never had before, and this power raises questions about our Fourth and First Amendment protections.

Police can't secretly fingerprint a crowd of people from across the street. They also can't walk through that crowd demanding that everybody produce their driver's license.

But they can scan their faces remotely and in secret and identify each person thanks to face recognition technology. Last year the Supreme Court in Carpenter noted that for the government to secretly monitor and catalogue every one of our movements across time and space violates our right to privacy, protected by the Fourth Amendment.

Face recognition enables precisely this type of monitoring. But that has not stopped Chicago, Detroit, and other cities from acquiring and piloting this capability.

The Supreme Court held in NAACP v. Alabama, Talley v. California, and others that the First Amendment protects the right to anonymous speech and association.

Face recognition technology threatens to up-end this protection. Law enforcement agencies themselves have acknowledged this, cautioning that the technology could be used as a form of social control, causing people to alter their behavior in public, leading to self-censorship and inhibition.

But that didn't stop the Baltimore County Police from using face recognition on the Freddie Gray protests in 2015.

Second, face recognition makes mistakes and its consequences will be borne disproportionately by African Americans.

One, communities of color are disproportionately the targets of police surveillance, face recognition being no exception. San Diego found that their police used face recognition up to two and a half times more on African Americans than on anyone else.

Two, people of color are disproportionately enrolled in police face recognition systems, thanks to being over represented in mug shot data bases that the system is run on.

And three, studies continue to show that the accuracy of face recognition varies depending on the race of the person being searched. Face recognition makes mistakes and risks making more mistakes, more misidentifications of African Americans.

A mistake could mean you are accused of a crime you didn't commit, like the Brown University student erroneously identified as one of the Sri Lankan bombers earlier this month.

One of this country's foundational principles is equal protection under the law. Police use of face recognition may not comport with this principle.

Third, left unchecked, current police face recognition practices threaten our due process rights. My research has uncovered the fact that police submit what can only be described as garbage data into face recognition systems, expecting valuable leads in return.

The NYPD submitted a photo of actor Woody Harrelson to find an unknown suspect in a beer theft. They have submitted photos of a suspect whose eyes or mouths have been cut and pasted in from another person's photo, essentially fabricating evidence.

Agencies submit drawings of suspects in places of photos as well, despite research showing that this will not work. Worse, officers at times then skip identification procedures and go straight to arresting someone on the basis of a face recognition search.

This practice runs counter both to common sense and to the departments' own policies. And these practices raise serious concerns about accuracy and the innocence of the person arrested because of a face recognition search.

But defendants are left in the dark about all of this, often never told that face recognition was used to help identify them. These systems produce Brady material—information that, under our constitutional right to due process, must be turned over to the defense. But it is not.

For all these reasons, a moratorium on the use of face recognition by police is both appropriate and necessary. It may be that we can establish common sense rules that distinguish between appropriate and inappropriate uses, uses that promote public safety and uses that threaten our civil rights and liberties.

But face recognition is too powerful, too pervasive, too susceptible to abuse to continue unchecked.

Thank you so much for your time. I look forward to answering questions.

Chairman CUMMINGS. Thank you very much.

Ms. Guliani?

STATEMENT OF NEEMA SINGH GULIANI, SENIOR LEGISLATIVE COUNSEL, AMERICAN CIVIL LIBERTIES UNION

Ms. GULIANI. Thank you for the opportunity to testify today on behalf of the ACLU.

Law enforcement across the country, including the FBI, continue to expand the use of face recognition without legislative approval, absent safeguards, and, in most cases, in secret.

It is time to hit the pause button. Congress must intervene to stop the use and expansion of this dangerous technology until we can fully debate what if any uses should be permitted by law enforcement.

I want to be clear. Use of this technology is already resulting in very real harms.

Chairman Cummings, in your opening statement you discussed the use of face recognition at the Freddie Gray protests in Baltimore and, like you, I share concerns about the impact on our First Amendment rights.

But it is not the only disturbing example. In Florida, there is the case of Willie Lynch, an African-American man arrested and convicted of a $50 drug sale. In his case police relied on a low confidence match of a poor quality photo that was secretly taken, and now Mr. Lynch cannot even get key information about the reliability of the algorithm used in his case so that he can challenge his conviction.

I want to highlight three reasons why I think it is particularly urgent that Congress act now and then offer two recommendations for areas where additional oversight is needed.

So why is this issue so urgent? One, we have never seen anything like this technology before. The U.S. reportedly has over 50 million surveillance cameras. This, combined with face recognition, threatens to create a near constant surveillance state.

Even more, right now police are often exploiting large-scale data bases like driver's license repositories for face matching. This im-

pacts the rights of everyone in these data bases, and we don't have the option of simply leaving our face at home to avoid being surveilled.

Two, this technology is more likely to harm vulnerable communities, including communities of color. Studies have found that face recognition is less accurate on certain subgroups including women and people with dark skin.

The ACLU tested Amazon's face recognition product, matching Members of Congress photos against 25,000 mug shots. There were 28 false matches including Representatives Gomez, DeSaulnier, and Clay, who sit on this committee.

Forty percent of the false matches were members of color. But even if this technology was 100 percent perfect, it is not being used in the perfect world. It is being used in the real world, and in the real world, poor communities and communities of color are over policed, they are more likely to be stopped, arrested, and to have force used against them.

These same disparities are likely to extend to the use of face recognition and heighten the risks associated for the errors.

Three, this technology is not being used consistent with the Constitution. Face recognition is potentially even more invasive than the warrantless tracking that the Supreme Court found unconstitutional in the Carpenter case.

Yet, it is being used without a warrant and without other protections. Additionally, the government is not complying with its notice obligations. Over a 15-year period where the Pinellas County Sheriff's Office used face recognition in investigations, the county public defender reported never once receiving information as exculpatory evidence, which is required by the Supreme Court's Brady decision.

As we debate this issue, we must do so with complete facts. Thus, I urge the committee to investigate two things. One, how is ICE, the FBI, and other Federal agencies using this technology?

When it comes to face recognition, the FBI has broken more promises than it has kept. It has not fully tested the accuracy of the systems it uses, nor does the agency appear to be complying with Constitution. Yet, the agency is now reportedly piloting Amazon's face recognition product.

ICE similarly has met with Amazon representatives and also appears to use CBP and State Department systems. But we know little else. The committee should examine these issues.

Two, the committee should look at companies that are aggressively marketing this technology to the government, including how accurate their technologies are and what responsibility they take to prevent abuse.

Companies are market this technology for serious uses like identifying someone during a police encounter, and we know far too little. For example, Amazon has even refused to disclose who it sells this technology to and companies like Microsoft and FaceFirst have so far not received significant congressional attention.

There are efforts across the country to stop this dangerous spread of this technology. San Francisco has banned the use by city departments and Amazon shareholders are today taking the unprecedented step of voting on a resolution that would stop the com-

pany from selling this technology to the government and force it to study the human rights impacts.

Congress should follow these good examples and put in place a moratorium on law enforcement use. I look forward to answering your questions.

Chairman CUMMINGS. Thank you very much.

Mr. Alexander?

STATEMENT OF CEDRIC ALEXANDER, FORMER PRESIDENT, NATIONAL ORGANIZATION OF BLACK LAW ENFORCEMENT EXECUTIVES

Mr. ALEXANDER. Good morning, Chairman Cummings and Ranking Member Jordan and——

Chairman CUMMINGS. I am sorry. Doctor. Doctor Alexander.

Mr. ALEXANDER. That is all right, sir.

Chairman CUMMINGS. After attending a number of graduations, I want to give you all your credit.

Mr. ALEXANDER. Yes, sir. Thank you very much.

Chairman CUMMINGS. All right.

Mr. ALEXANDER. And distinguished members, thank you for me having the opportunity to be here with you this morning. I am going to speak from the perspective of a 40-year police veteran, Chairman, someone who has led organizations both at the local state and Federal level.

Based on a 2016 investigation by Georgetown Law Center on privacy and technology, at least a quarter of U.S. law enforcement agencies use facial recognition searches of their own data bases or those of other agencies in an attempt to identify, find, and arrest criminal suspects.

As of 2016, at least 16 states permit the FBI to use the technology to compare suspects' faces with images of state-issued IDs. Now, sometimes law enforcement uses facial recognition prudently and wisely, sometimes recklessly.

On May 16, the Washington Post report that some agencies use altered photos, forensic artist sketches, and even celebrity look-alikes for fake facial recognition searches. Using artificial intelligence to confer on a highly subjective visual impression a halo of digital certainty is neither fact-based nor just.

But it is not illegal, for the simple reason that no Federal laws govern the use of facial recognition. At this point, law enforcement use of facial recognition is not only unregulated by law, it operates even without any consensus on best practices.

Artificial intelligence systems do not invent results from thin air. They operate from data bases of identified faces in an attempt—an attempt to match one of those identified faces with the face of a suspect or subject of interest.

An artificial intelligence system is only as good as its data bases. Yet, there is currently no standard governing the content of any agency's facial images data base.

Who is included in it? Who knows. What we do know is that publicly available facial data bases fail to represent the size and diversity of the American population and are therefore inherently biased samples.

Real-time video surveillances can identify criminal activity in progress. But for the purpose of investigation, what are the risks to Fourth Amendment guarantees against unreasonable search and seizure?

And the legal standards should be required prior to facial recognition search. Answer—we don't know. And before we leave the Constitution, is there a basis to fear that the combination of widespread real-time video surveillance and spatial recognition, AI may infringe upon the First Amendment protection of free speech, assembly, and association. So far, this remains unanswered, barely even addressed.

How accurate is facial recognition technology? The answer is it depends, and that is an unacceptable answer for law enforcement, the justice system, and the people of this country.

Facial recognition works best from images and bright even lighting. Identifying partially turned faces of those poorly lit is like trying to read a badly smudged latent fingerprint.

Real-time video surveillance often supplies poor quality images and result in erroneous identifications. One of those things that artificial intelligence would preclude a racial and other biases.

In fact, the New York Times reported in February of last year facial recognition algorithms marketed by major software suppliers in this country were significantly more likely to misidentify the gender of black women than white men.

Gender was misidentified up to 1 percent of the time in the case of light-skinned males and 35 percent of the time in the case of darker-skinned females.

The problem with artificial—AI skin color bias is serious enough that a CBS report—news report on May 13 San Francisco is considering a citywide ban on facial recognition in all government agencies.

Now, this seems to me to be an overreaction. But considering the current absence of law, regulations, or even generally agreed upon best practices, it is certainly an understandable overreaction.

We human beings are hardwired by evolution to fear and suspect danger when confronting the unknown. The opaque, even secretive attitude of law enforcement with regard to facial recognition plays into that primal fear.

The Georgetown Law Center on Privacy and Technology reports that defense attorneys have never received face recognition evidence as part of a Brady disclosure that—which legally which is that many of us know legally it is required disclosure of exculpatory or impeaching evidence that may prove the innocence of a defendant.

Only a very small minority of law enforcement agencies disclose how, and how frequently, they use facial recognition. Very few agencies even claim to audit their personnel for improper use of facial recognition systems.

Indeed, the vast majority of agencies do not have any internal oversight or accountability mechanisms to detect misuse. Neither Federal, state, nor most local governments subject police policies concerning recognition to legislative or public review.

Secrecy in matters of constitutional rights, human rights, and civil rights provoke fear and suspicion.

And last, like so many digital technologies, facial recognition was long ago—not long ago the stuff that we saw as being science fiction. Today, many of us carry in our pockets in the form of a smart phone that recognizes our face when we take it out to make a call or send a text.

It has become a normal part—a normal part of 21st century living and most Americans have no problem or not trouble accepting that facial recognition can be a valuable tool in law enforcement.

But without the judicious and just application of human intelligence including full disclosure, transparency, public accountability, prudent legislation and science-based regulation, the technology of artificial intelligence do not deserve to be called tools.

They are, instead, blunt instruments and in the worst cases blunt instruments become weapons.

Thank you very much.

Chairman CUMMINGS. Thank you very much.

Ms. Hill?

Ms. HILL. Thank you, Mr. Chairman, and thank you to all of you for being here. This is of particular interest to me because one of the communities in my district is planning on implementing facial recognition technology in its city within the coming months with thousands of cameras across the community.

In Carpenter v. the United States, the court found that police violated the Fourth Amendment when they collected cell phone location data without a warrant.

In that case, Justice Alito, in a dissent, wrote that Congress is a better arbiter of controlling lawful use of new technologies by police than the courts.

Justice Alito wrote, "Legislation is much preferable to the development of an entirely new body of Fourth Amendment case law for many reasons, including the enormous complexity of the subject, the need to respond to rapidly changing technology, and the Fourth Amendment's limited scope."

Ms. Garvie, can you speak to how quickly facial recognition technology is developing?

Ms. GARVIE. I can. Face recognition is developing incredibly fast. We must caution, though, against anyone who says that these algorithms are getting better, which means that the results of the systems will be getting better, because as we have seen, it doesn't matter how good an algorithm gets. If law enforcement agencies put unreliable or just wrong data in, they will not get reliable results out. These algorithms are not magic.

Ms. HILL. Thank you.

And Professor Ferguson, do you think the Supreme Court can rule quickly enough upon the use of these technologies as the cases arise to thwart constitutionally questionable uses?

Mr. FERGUSON. They can, but they won't do as good a job as Congress regulating it now. Justice Alito has repeatedly made that claim and I think he is correct to say that this kind of technology should be regulated first by Congress. The Fourth Amendment floor will exist and the Supreme Court will address it. But this body has the primary responsibility to regulate in this field.

Ms. HILL. From your testimonies and your answers right now, it sounds like there is broad agreement that Federal legislation is

necessary in order to prevent a confusing and potentially contradictory patchwork of regulation of government use of facial recognition technology.

Just last week, San Francisco passed an ordinance barring police and other government agencies from using facial recognition technology. San Francisco's decision has attracted attention across the country and could be followed by moves from other local governments and at the same time we have local governments that are adopting this.

The drafter of the San Francisco ordinance is pushing for additional bans in Berkeley and Oakland and a proposed Massachusetts state bill would ban government use of facial recognition systems.

At the same time, many states have also partnered with the FBI to grant access to their collection of driver's license photos for use in face image searches. Needless to say, the maze of recognition across cities and states can be confusing to navigate.

Citizens may be afforded certain protections from warrantless surveillance through the use of facial recognition in one state but then drive several miles and be subject to a completely different regime.

Ms. Guliani, can you discuss the range of different standards we see across states?

Ms. GULIANI. I think by and large, when we are hearing from communities it is with a great deal of anxiety about face recognition. When communities know that this is being used, they are raising concerns that it has been done without community input, without clear rules, and without the right standards to protect First Amendment and other—you know, and other core values.

So I think the trend is definitely in that direction. But I think, you know, one of the important things of this hearing is to ask the questions and have the debate, and until we do that we just shouldn't be using that technology for all of the concerns it raises.

Ms. HILL. So if we are talking about a local government or another company or agency that is looking to implement something like this, what advice would you give at this point, given the lack of guidance—and I guess this question goes to all of you—and what recommendations do you have for us in this body to move quickly and to be able to set sort of a baseline of—you know, how local governments should operate at this stage?

Ms. GULIANI. I mean, the advice I would have is to not use the technology until there has been a legislative process and clear standards and rules. And you have seen this sort of pop up in a lot of cities around the country. It is called Community Control Over Policing Surveillance, right.

This idea that we shouldn't put the cart before the horse. We should study the harms before you rule something out. That would be my greatest recommendation and I think that we should do that federally as well with this technology.

Ms. HILL. Anyone else want to weigh in?

Ms. GARVIE. I would add that most state and local law enforcement face recognition systems have been purchased using Federal grant money, which means Congress has incredible power to actu-

ally decide how much transparency goes into implementing these technologies and what rules are in place as well.

Mr. FERGUSON. I think Congress has a role to set the floor and allow local governments and cities to build off that so you can have places like San Francisco. I think we have seen real leadership in local cities about democratic control over surveillance technologies.

But I think that that is no reason not—to not have Congress also act.

Ms. HILL. Thank you. And I know I am out of time, but will you be able to provide us with recommendations for that floor as kind of a follow-up to this?

Mr. FERGUSON. Yes. I attempted to do so in my written testimony and would be happy to work with the committee, going forward.

Ms. HILL. Thank you.

I yield back.

Chairman CUMMINGS. Thank you very much.

Mr. Jordan?

Mr. JORDAN. Thank you, Mr. Chairman.

Ms. Guliani, facial recognition system makes mistakes and those mistakes disproportionately impact African Americans and others of color. A facial recognition system appears to me to be a direct violation of Americans' First Amendment and Fourth Amendment liberties and a facial recognition system also seems to me to threaten, as Ms. Garvie said, Americans' due process rights.

And all three of those things—all that happens in a country with 50 million surveillance cameras. Is that accurate?

Ms. GULIANI. That is correct.

Mr. JORDAN. How does the FBI get the initial data base in the first place?

Ms. GULIANI. So the FBI has massive data bases and they use external partners as well. So one of the things they do is they use state driver's license data bases. I think, you know, up to 18 states have been reportedly used by the FBI. They use passport photos.

Mr. JORDAN. Who made the decision to allow the FBI to access those 18 or 19 states' DMV data bases?

Ms. GULIANI. Apparently there were conversations and memorandums between those states. But in one state, for example in Vermont, it was actually against state law and ultimately the attorney general had to suspend that use.

Mr. JORDAN. So my question is, again, did the state legislature and the Governor actually pass legislation saying it was okay for the FBI to access every single person in their state who has a driver's license? Did that happen in those 18 or 19 states that gave that permission to the FBI?

Ms. GULIANI. No, and that is the problem. This was all in secret, essentially.

Mr. JORDAN. So some unelected person at the FBI talks to some unelected person at the state level and they say yes, go ahead—here is—in the case of Ohio we have got 11 million people. Most of them drive. Here is 10 million folks who you can now have their—have this data base?

Ms. GULIANI. Right, and the people who wanted a driver's license many times didn't know these systems were operating either.

Mr. JORDAN. That was my next point. And the individual themselves did not get permission. Is that right?

Ms. GULIANI. That is exactly right.

Mr. JORDAN. So the individual didn't get permission. Were there any kind of notifications at the time they go in to get their picture and get their driver's license, oh, at my four years I got to get my new tag, my—or my new license—any type of information given to them, oh, by the way, this may go to the FBI?

Ms. GULIANI. You know, I think by and large people have been unaware of these systems and how they operate.

Mr. JORDAN. So the individual is unaware. The people they elect to represent them in their state government did not make the decision. That information is going to the FBI, which scares me, particularly in the context of—I mean, you can use your examples.

Some people would say do you really want J. Edgar Hoover having this capability. I would argue today do we really want someone like Peter Strzok with the things we have learned that he engaged in and the bias that he had, and no one—no one in an elected position made the determination?

Ms. GULIANI. That is right.

Mr. JORDAN. Okay. Now, when the FBI has this and they are going to access this data base, what kind of standard do they have to put in place before they can access it? Is there any type of probable cause?

Any type of—any type of process, due process, whatever you want to call it? Anything they go through before they can access the data base?

Ms. GULIANI. They don't have to get a warrant or meet a probable cause warrant standard, and I think there are questions that they aren't even notifying people in cases where it is relevant in their case.

Mr. JORDAN. Okay. Fifty million cameras, violation of people's First Amendment, Fourth Amendment liberties, due process liberties, all kinds of mistakes.

Those mistakes disproportionately impact African Americans, and no due process. No elected officials gave the okay from the states for the Federal Government or the FBI to use it.

Does the FBI share any of this information with other Federal agencies?

Ms. GULIANI. They have partnerships with Federal agencies, for example, like the State Department to scan through their passport photos.

But, frankly, we don't know very much about how other Federal agencies are using——

Mr. JORDAN. Do we know if the IRS has access to this kind of information? Can they—do they have any kind of partnership with the FBI or any other Federal agency to access this data?

Ms. GULIANI. I don't know the answer to that question with regards to the IRS.

Mr. JORDAN. That scares me—scares me as well.

So I guess the fundamental question is I think you are all there. There should probably be some kind of—some kind of restriction.

Mr. Ferguson, I think you have said we should just ban it, right?

Mr. FERGUSON. I think we should ban face surveillance, which is the use of these technologies without any kind of individualized suspicion and I think there should be regulation about face recognition technologies in certain ways.

But I do think that there are members of this panel who believe that at this moment there should be a moratorium, and, again, my position is if we are not going to regulate we should push the pause button on this technology now because it is as dangerous as you are expressing.

Mr. JORDAN. Seems to me it is time for—it is time for a time out. Time out. Fifty million cameras, real concerns. I guess what troubles me too is just the fact that no one in an elected position made a decision on the fact.

These 18 states—I think the chairman said this is more than half the population of the country. That is scary, particularly in light of what we see. You got to remember the framework.

It was just, what, eight years ago the IRS targeted people for their political belief. They did it. We know what—you can—it doesn't matter what side of the political spectrum you are on. This should concern us all and this is why I appreciate the chairman's work on this issue and the bipartisan nature of this hearing.

With that, Mr. Chairman, I yield back.

Chairman CUMMINGS. Just to clarify what the ranking member said, Ms. Buolamwini, you were recommending a moratorium. Is that right?

Ms. BUOLAMWINI. Yes, I was.

Chairman CUMMINGS. Until what? Until what? Until we can pass legislation? Is that it?

Ms. BUOLAMWINI. Until there is sufficient scientific evidence that shows that these technologies have reached maturity, because with what we know with human-centric computer vision systems, as they are based on statistical methods, there is no way that the technology will be 100 percent flawless and there are tradeoffs that need to be made.

Yet the academic research just doesn't yet exist to say this is what it looks like for it to meet meaningful thresholds.

Chairman CUMMINGS. All right.

Yes, Ms. Norton?

Ms. NORTON. Thank you very much, Mr. Chairman, for this hearing.

I must say I think we are already a little bit pregnant and I agree with the ranking member, and we have got these cameras everywhere. We are a little late in saying, well, you really shouldn't be surveilling people when there is nowhere that we don't surveile people.

I thank Ms. Guliani. I remember the ACLU when we first began to surveile people raise the issue of, you know, is this really constitutional? Is this really right? I don't know if it was—it was ever challenged and got to court.

I must say this takes me back to my days as a law professor because all kinds of hypotheticals occur to me.

I got to ask you, Mr. Ferguson—maybe Ms. Guliani—is there a difference between misidentifying people using facial technology

and misidentifying people which happens all the time so that the police draw in people based on people saying, that is who I saw?

What is—what is the difference? How are we to argue that in court?

Ms. GULIANI. Sure. I mean, I think one of—the big difference is—differences is with an eye witness you can put them on the stand and you can say, look, were you 800 feet away? Were you intoxicated?

With algorithms, defendants aren't getting information about the algorithm. They can't put them on the stand in the same way and a lot of times this technology is being presented as if it is perfect when it is not.

Ms. NORTON. Let me ask you about police encounters. Suppose the police stop you for speeding. Now, there is some probable cause there. He saw you. You can contest it.

Can he put your photo in a data base that the police have having already had probable cause to stop you? Can he take your picture and say, okay, you can show up in court but this is for our data base?

Mr. FERGUSON. Right now, the police officer can because there is no regulations on any of this. The concern is that that may not be the way we want to go forward and might be a reason to actually have this kind of regulation.

That is a use. There are companies that literally sell that technology for that reason and it is, again, a reason to act.

Ms. NORTON. I raise that—I raise that hypothetical—a law professor's hypothetical because I think we are already doing what we are already afraid of and that we ought to look very closely at regulation. Watch out because you will be regulating stuff that is already done by law enforcement and that nobody—and that we have given a pass to.

I wonder, Professor Ferguson, if you have any sense of how, particularly since there has been recent Supreme Court—Supreme Court decision on cell phone location data, any sense how today's conservative Supreme Court would rule on facial recognition technology.

Mr. FERGUSON. I think in certain uses when you are talking about a system of cameras that can track where you go, the principles that the Supreme Court, including Chief Justice Roberts, was concerned about, this idea of tracking, this idea of aggregating personal information, this idea of the permanence.

So you can go back and look and see where people have gone because this footage is available and you can track where you have been at every moment. This idea that we don't like arbitrary police powers or permanent police powers all speaks to the fact that the Supreme Court, if faced with the right case, might see this as a Fourth Amendment violation.

Unfortunately, these cases take a long time to get there. Unfortunately, that it would be, you know, relying on the Fourth Amendment may not be the place we want to be and I think that Congress has the opportunity to act now to sort of forestall our reliance on any number of the Supreme Court justices.

Ms. NORTON. Particularly in light of the issues raised by the ranking member, I mentioned that this monitoring—he mentioned

this monitoring by facial recognition has been done really on a mass scale over time and we have let his happen.

Can this—do you think that there is a violation of the Fourth Amendment if in doing the very monitoring that is done now, for example, if you go—if we have inauguration on the Mall, that monitoring is done all the time. That is monitoring or the use of technology on a mass scale.

If it is done over time and it is a part of regular surveillance for the safety of those involved, do you think the court would see that monitoring over time as unconstitutional?

Chairman CUMMINGS. The gentlelady's time has expired but you may answer the question.

Ms. GULIANI. I mean, I think the Supreme Court's Carpenter decision is applicable to some of the uses of face recognition. Like when you mentioned tracking people over long periods of time, I think in that case the court said that warrantless tracking of that nature was unconstitutional and I think that there are also significant First Amendment concerns, for example, if there was a policy of identifying every single protestor every time they went to a protest, right.

I do think that there is strong case law that would raise constitutional concerns with that. But, fundamentally, you know, the Carpenter case was decided two decades after we all started using cell phones.

So it takes time for these things to work through the system and it is harder when people aren't receiving notice so that they can raise these concerns to judges.

Chairman CUMMINGS. Mr. Alexander, I noticed that you were trying to answer the question, too. Were you trying to answer the question?

Mr. ALEXANDER. Yes. To Congresswoman Norton, you know, the question you raise is a very good one so I am going to respond to it from a law enforcement perspective.

Ms. NORTON. Thank you.

Mr. ALEXANDER. For me, and I am quite sure for many of my colleagues across the country, this technology that we are referring to can be very valuable in terms of keeping our communities and keeping our country safe.

There are opportunities for that. The problem that has occurred it is kind of like the horse that have already gotten out the gate and now we are trying to catch up with it, because if you think about the vast utilization of facial recognition that is going on and the questions that we are posing today are going to come with a great deal of challenges.

I kind of cringe in some ways when I hear my colleagues here respond to maybe there should be a complete halt—a moratorium on facial recognition. I am not sure if that is the answer.

What I am more concerned about is the failed use and the misuse of the technology and how do we acknowledge that and how to we differentiate between when it is being used correctly and what it is not.

But here is the problem I have for policing in this country as it relates to this technology. The police end up being the end user of

a technology that is created by some software technology firm somewhere.

I go out. I use the technology. If I am not properly trained, if I am not properly supervised, if there is no policy, there is no transparency that I am sharing with people in my community about how and when this technology is being utilized and then something goes awry, then I, the end user—that police chief, that police department—end up being the bad guy, and God knows that is one thing that policing don't need, considering the environment that we are already in trying to build relationships between police and community.

So there is a place for this technology. But I think, more importantly, to me and I am quite sure for many of my colleagues that are out there is that I need to be able to make sure that I can train my people adequately.

These software companies need to not just pass this technology to me; I need to be sure that my folks are trained. There is ethics. There is morals that goes along with it. There is policy. There is standards. There is good practices that we know and we feel good about.

But I am not certain if a total moratorium in light of the fact that we still live in an environment where we are under a great deal of threat we still can utilize this technology. But it has to be in a way right now how do we do that while work trying to develop some standards.

Chairman CUMMINGS. Thank you very much.

Mr. Cloud?

Mr. CLOUD. Thank you, Mr. Chairman, and Mr. Chairman, let me first of all say thank you for holding this hearing. This is an extremely important topic and the concerns the ranking member laid out I couldn't have said them any better, the concerns of information being shared without any sort of accountability by people who represent—who are elected to represent them.

This is scary. I mean, we heard the stories about China, how China is already using this technology to target Muslims and Christians. We have known our own abuses recently in our own government of how agencies have gone—as was mentioned, the IRS, FBI recently.

I mean, this is real scary stuff. Dr. Alexander, I liked your analogy of the horse and getting out of the gate too quick. I am of the tendency of let us air on the side of liberty while we don't know what is going on here.

But in your thoughts, and maybe, Mr. Ferguson, if you can add to this, when would be limited appropriate use and at what point do we need to have the technology developed?

Mr. ALEXANDER. Well, I mean, for me, you know, that is a very tough question. But I think this hearing and the hearings that are going to follow, and maybe even some smaller sessions particularly with our Federal law enforcement, i.e., FBI, who utilizes this technology to fight off potential threats on a much larger scale, I think when you start talking about local policing in and of itself I think to have an opportunity to talk to some of the chiefs across the country in terms of how they are using this technology and how they think it could best benefit them if we can develop some lim-

ited framework in which they can operate from and maybe not as vast that it is now because it certainly is a serious issue and concern and problem that we have.

It is not as transparent as it should be and it certainly is going to create a great deal of angst and anger among Americans in this country and particularly people who are—who are—their First and Fourth Amendments are violated.

Mr. CLOUD. Sure.

Mr. ALEXANDER. And we are going to find ourselves in this kind of position where we don't want to be. So I think this is going to require further conversation certainly beyond today. But it is something that we have to act on now in a temporary basis.

But I am not sure if a total moratorium on this is going to be the answer to us because we still have a homeland we have to protect and there is still some value in facial recognition.

Mr. CLOUD. Thank you.

Mr. Ferguson?

Mr. FERGUSON. In my written testimony I lay out what I think can be the way to regulate this, which involves a probable cause plus standards sort of based on the Wiretap Act, requiring an assertion of probable cause and a sworn affidavit to be able to use and search the data base for facial recognition, care to minimize the unintended collection because there would be other faces in this, the memorialization and documentation of how it is used so you could answer those questions about whether it had been used and by whom, and steps to make sure that there was a process in place to see what had happened and be able to check if there are abuses.

Mr. CLOUD. Thank you.

Ms. Buolamwini—did I say that right?

Ms. BUOLAMWINI. Yes, you did.

Mr. CLOUD. Okay. You mentioned Facebook in your remarks and I find that interesting because I am extremely concerned about the government having this kind of unchecked ability. I would be curious to get your thoughts of corporations having this same sort of ability.

And also, Ms. Garvie and Ms. Guliani, if you want to speak to that, too.

Ms. BUOLAMWINI. Absolutely. So you are looking at a platform that has over 2.6 billion users and over time Facebook has been able to amass enormous facial recognition capabilities using all of those photos that we tag without our permission.

What we are seeing is that we don't necessarily have to accept this as the default. So in the EU where GDPR was passed because there is a provision for biometric data consent, they actually have an option where you have to opt in.

Right now we don't have that in the U.S. and that is something we could immediately require today.

Ms. GULIANI. I mean, just to add to that, it is certainly something where Federal legislation is needed. We can look to the state of Illinois for sort of biometric laws. They have a law on the books requiring consent to use biometric information.

But very importantly, they also have a private right of action. So if Facebook or any other company violates my rights and uses my

face image without my permission, I can take them to court, and that is a really important accountability mechanism.

Ms. BUOLAMWINI. The other point to bring up is the fact that oftentimes data is collected for one use and then ends up in another scenario.

So a recent example of this is with Ever, a photo sharing company, where users uploaded images of their kids and, you know, graduations and so forth, and later on they found out that those photos were used to train facial recognition that the company now sold as Ever AI.

So we definitely need data protections when it comes to the use, disclosure, and consent around biometric face data.

Mr. CLOUD. Thank you, Chairman.

Chairman CUMMINGS. Mr. Clay?

Mr. CLAY. Thank you, Mr. Chairman, and thank the witnesses for being here.

You know, the use of facial recognition technology has already generated a heated debate on whether it is a necessary tool to combat crime or an unlawful breach of privacy.

The technology identifies people's faces and runs them against a watch list of images which can include suspects, missing people, and persons of interest. But privacy campaigners have described the technology as Orwellian.

I was allegedly misidentified using this technology along with 27 other Members of Congress—disproportionately black and brown members.

So I have questions about the accuracy that protections against misidentification and, obviously, civil liberty issues.

Ms. Guliani, I want to hear more from you about the testing of Amazon's recognition software. The ACLU alleges Amazon software incorrectly matched Members of Congress, identifying them as people who had been arrested for a crime.

If Members of Congress can be falsely matched with a mug shot data base, what should be the concern for the average American about the use of facial recognition?

Ms. GULIANI. Sure. I mean, with regards to the tests, I think that one of the most interesting thing was that running the test cost us less than a large pizza. It was about $12.

And we took photos of Members of Congress, really ideal conditions, right—portraits—matched them against mug shots and we found those 28 matches. These were independently verified.

And I think that one of the things that is important to note is it is not just our test. It is other tests that have noted similar problems with Amazon software and other face recognition algorithms.

Now, we just ran a test. But imagine this in the real world. Imagine you are arrested or convicted or you are pulled over by police and you are—they say, we identified you as this person, you don't even have the information to say, look, you are wrong—the algorithm got it wrong, and that is really the nightmare scenario that we are worried about and why we think that, you know, the prudent thing to do would be to hit the pause button.

Let us get the information out there, understand the dangers, understand whether this technology is really the helpful—the way people say it is and then let legislatures like this decide.

Mr. CLAY. Let me ask you, has the ACLU shared its methodology on data sets used for the test of Amazon's recognition that resulted in false matches with criminal mug shots?

Ms. GULIANI. We had it independently verified by a Stanford professor. We elected not to release the mug shot photos for the privacy of those individuals. We didn't want to have their photos, you know, in newspapers, et cetera, when they were not, you know, public figures.

Ms. BUOLAMWINI. But I can say the Algorithmic Justice League, we tested Amazon recognition using the same methodology that we tested IBM, Microsoft, Face++.

Our data set is publicly available under the right license. Our methodology came from my MIT thesis and was available over a year before we tested Amazon and also found that they had false—they had error rates of over 30 percent for darker-skinned females and zero percent error rates for lighter-skinned men.

So it is the case that there is verifiable research that shows you have issues with Amazon recognition.

Mr. CLAY. And has any of that been corrected in the lab or through their technology?

Ms. BUOLAMWINI. So what we found with the first studies we did of IBM and Microsoft is that they did improve their accuracy disparities. But even when they approved they still performed better on men's faces than women's faces. They still performed better on lighter skin than darker skin. So even when it is closing we still see a bias.

Mr. CLAY. And, Doctor, you know what the collateral damage can be through misidentification and I have fought for years to free people from prison who were wrongfully convicted and that is where this is going because of lax rules and regulations and technology.

Ms. BUOLAMWINI. Absolutely, and we don't even have reporting requirements. At least in the U.K. where they have done pilots of facial recognition technology, there are reported results and you have false positive match rates of over 90 percent. There is a Big Brother Watch U.K. report that came out that showed more than 2,400 innocent people had their faces misidentified.

And so this is building on what ACLU said, right. We already see this in the real world where performance metrics are required. We don't have any kind of requirements in the United States.

Mr. CLAY. All in the name of profits.

Mr. Chairman, my time is up. I yield back.

Chairman CUMMINGS. Before we go to Mr. Massie, let me say this. As I listen to this testimony I am troubled by something you said, Dr. Alexander.

It seems like we have a defective system. It is defective, and it—and so when you say that you are not—that it has good purposes, it also can be extremely harmful.

And when you balance people's rights, that is a problem. I mean, so I don't know—in the law we constantly are trying to do a balancing act with law enforcement and everything.

But when you guys have a product that is defective and reading wrong, that is a problem, and it has a chilling effect on our total

population. I just want you mull over that because I am going to come back to you when I have my question.

Mr. ALEXANDER. Yes, I would like to respond to that.

Chairman CUMMINGS. Yes. I am going to come back to you.

Mr. Massie?

Mr. MASSIE. Thank you, Mr. Chairman.

The Supreme Court case, Brady v. Maryland, held that the government is required to release to the defense potentially exculpatory evidence that they come upon when prosecuting the case and I am worried that facial recognition technology presents a threat to that.

For instance, Ms. Guliani, if multiple photos are returned during a search of the data base to the FBI and they narrow it down to a single suspect, are they—does Brady require the FBI to share those other photos that were similar to the suspect in question?

Ms. GULIANI. Yes. I mean, certainly it could be exculpatory evidence to know, for example, that an algorithm has a reliability problem or that an algorithm returned, you know, similar photos with—indicating they can be the person.

That could support a defense to say, look, I have been misidentified—there were other people who were similarly tagged by the system.

And I think that one of the concerns is that we are not seeing Brady disclosures and we are not really seeing notice. The FBI has used this stuff hundreds and thousands of times. There aren't thousands of cases in the court where we see defendants being informed about this. So judges are not having even the opportunity to rule on some of these very critical issues.

Mr. MASSIE. Well, one of the concerning things too is that when a human makes a identification or a false identification you can cross-examine the human—were they drunk, was it dark outside, how was their vision, do they have prescription glasses, were they wearing them—all of those things. But you can't cross-examine an algorithm.

Ms. Garvie or Ms. Guliani or Mr. Ferguson—anybody here—has the government been providing descriptions of how the algorithms work to the defense? Anybody?

Ms. GARVIE. They have—they have not. In speaking to public defenders around the country we have found that they will usually not know if the algorithm was used in the first instance.

Law enforcement agencies don't typically have access to the training data or to how the algorithms work as well because these are private companies that have developed these systems, and it is considered a trade secret. So it may be that the law enforcement agency says they can't turn over. So we have not seen public defenders having access.

On your point about Brady, face recognition systems are designed to return multiple matches. The Washington County Sheriff's Office gave an example where a person—a person with a 70 percent confidence was the person they ended up charging, even though the algorithm thought somebody else was at a 90 percent confidence.

Essentially, the algorithm was playing witness, saying that I am 90 percent confident it is this other guy, and yet the person who

I am 70 percent confident is the guy was the one who was charged. That it quintessentially Brady evidence.

Mr. MASSIE. I have got a couple minutes left. I want to pivot a little bit. We have talked about in the cases where facial recognition doesn't work, and it is very concerning, especially when it disproportionately affects minorities when these algorithms are defective.

But I am worried about the case where they work 100 percent of the time where there are mistakes and nobody gets left out. Ms. Garvie, can you speak briefly to how China is using real-time facial surveillance?

Ms. GARVIE. Sure. We see China as a bit of a roadmap of what is possible with this technology in the absence of rules, and in the absence of rules this is a system where everybody is enrolled in the back end and there are enough cameras to allow law enforcement to track where somebody is anytime they show their face in public, to upload their photo and see where they have been over the last two weeks, be that public rallies or an Alcoholic Anonymous meeting or a rehab clinic.

That information is now available at the click of a button or the upload of a photo. That is what face recognition looks like with no rules.

Mr. MASSIE. So do we have any evidence that any U.S. police departments or Federal agencies are doing real-time monitoring of events or large events or using streams from cameras and monitoring them today?

Ms. GARVIE. Our research has found that at least two major jurisdictions—Chicago and Detroit—have purchased this capability and have paid to keep—to maintain it.

Chicago says they do not use it. Detroit did not deny that they were using it. Theirs is designed to operate with Project Green Light, which is specifically locations like, yes, gas stations and liquor stores but also churches and clinics and schools.

Mr. MASSIE. Is there a minimum threshold of evidence or suspicion that is required before your face becomes one of the faces searched in real time or in one of these data bases—I mean, presently?

Ms. GARVIE. In no—in no jurisdiction there are rules around who ends up in the data base with few exceptions. In Missouri, for example, DMV records cannot be included. But, by and large, there are no rules around this.

Mr. MASSIE. Thank you very much, Mr. Chairman. I yield back the balance of my time.

Chairman CUMMINGS. Mr. Rouda?

Mr. ROUDA. Thank you, Mr. Chairman.

And I agree with you, Mr. Chairman. This is a difficult discussion as we try to balance our private rights with the potential proper use of facial recognition technology.

I want to focus on three different areas, and the first one is getting the sense from the panel here are there some of you who believe that we just outright need to stop this technology from being used versus legislation on proper use?

A second area I would like to talk about it is if we do agree proper use makes sense, some sort of definition around that for law en-

forcement versus private use, and then finally maybe talking about if there are violations of that proper use what we would consider appropriate penalties.

So let us start with that first area, and I ask the whole panel is there anybody on the panel that flat out says that we need to stop this technology in its tracks as is, period?

Ms. BUOLAMWINI. Well, it definitely depends on the kind of technology we are talking about. So we not only have facial recognition being used by law enforcement. We have broader facial analysis capacities now being used in employment.

A company called Higher View purports to do video analysis on candidates for a job to pick up verbal and nonverbal cues and they train on the current top performers within a particular company.

There is a case where an Uber driver just had their account deactivated because Uber uses a face verification system to determine if you are actually the driver, and just last year you had transgender folks who were also kicked out of Uber because of these misidentifications.

So that is a use case that is beyond law enforcement where I wouldn't necessarily say it is a flat out ban. But we need to be very specific about which use cases we are talking about.

For law enforcement, as it stands right now I absolutely think there should be a moratorium because the technology hasn't reached maturity and we don't have regulations.

Mr. ROUDA. Did somebody else want to speak to this as well?

Ms. GULIANI. Certainly. I mean, I think I would say two things. One, there are going to be uses of this technology where we are going to want a flat-out ban, right—real-time tracking, use in protests, use in sensitive areas.

And two, I think to determine what, if any, uses are permissible, we need the facts. You know, we referenced a U.K. study where there was a 95 percent inaccuracy rate. To me, that is a very relevant question as to whether we want this type of technology being used by law enforcement at all.

So until we have those facts, I think it is hard to answer all the questions.

Mr. ROUDA. And that is a fair statement. My concern is that bad actors are always going to use the tools that they can access, and if they can access these tools even though we want to prohibit it from happening, they are going to access it.

So my sense is better that we need to figure out what is the proper legislation for proper use of it and if we do move to that question—proper use, law enforcement versus private—law enforcement has been using digital enhancement of photos for years and years and I don't think anybody is suggesting that that is stepping over the line. There was mistakes that are made all the time as well.

And so my question is how do we make sure that law enforcement, in using this technology, is using it in the proper way?

Mr. ALEXANDER. Well, let me respond to that, and I think to your question—your first, second, and third question, quite frankly, because there is a string that goes between them—and it goes back to what I was saying at the beginning of this is there may be a

place for law enforcement to be able to utilize technology—this technology.

The problem is, is that the technology is developed by a software company. It is sold to a police department without proper training, without proper understanding by that department the utilization of it, and the unintended consequences.

That becomes a real problem. We have to be able to train. We have to be able to understand the technology. We know that this technology has been given to police and when police were asked to describe how it is used they couldn't do so. That is a problem.

And therefore, no, they should not be utilizing this technology. But going back to a question that was asked a moment ago, are there—are there times or have there been opportunities when this technology has proven to be valuable for law enforcement to keep communities safe.

The problem is here is that we are trying to keep the communities safe, at the same time trying not to violate people's First and Fourth Amendment rights.

They will rub up against each other and we somehow have to figure this out. But I don't think you can do one—just throw one out and just get—you can't throw the baby out with the bath-water is what I am trying to say.

Mr. ROUDA. Another quick question. Does this—does this technology—we see that there are mistakes. Is there a greater propensity for mistakes with the current technology than previous technologies, whether it is artist's renderings or photographs in general?

Ms. GULIANI. I think the concerns are different. You know, we have talked about how law enforcement can identify you from far away, right, in a traditional scenario where somebody asks me for my ID felt that it was harassment. I knew somebody was asking me for that information.

I could have raised a complaint. And, frankly, the community would know and be able to raise that with their elected leaders.

I think the secrecy of this technology is different. The scale is different. The cheapness is different. And so we have to address, I think, those fundamental threats before we can sort of talk about what are or aren't good uses.

Mr. ROUDA. Thank you, Mr. Chairman. I yield back.

Chairman CUMMINGS. Thank you.

Mr. Comer? Mr. Comer?

Mr. COMER. I just wanted to ask a couple of questions about facial recognition technology reforms. First question to Professor Ferguson. Should states and localities be able to enact their own facial recognition technology laws?

Mr. FERGUSON. I think the Federal Government should set the floor and I think that states and local governments can raise that floor and create more protections.

Mr. COMER. Okay.

Ms. Guliani, you testified that state and local governments have taken steps to ban or limit facial recognition. Could you speak on what those efforts look like across the spectrum?

Ms. GULIANI. Sure. In San Francisco, there was a recent vote to ban the use of face recognition by city governments. In Washington

and Massachusetts, there have been—there has been legislation introduced that would put in place a moratorium to study the technology and not permit use until that study is complete.

And there are 13 localities that have put in place measures that essentially require that before surveillance technology is deployed, like face recognition, there has to be a public process. It has to be voted on by the legislature and there need to be assessments to look at the privacy and civil liberties impact.

Mr. COMER. So does all the panel agree that the Federal Government needs to set the floor before states and localities create their own rules and regulations with respect to this? Is that a consensus among everyone on the panel? Yes or no.

Mr. FERGUSON. I am not sure before. I think they both need to act because it is that serious. Both states and locals and the Federal Government need to act quickly.

Mr. COMER. Okay. All right.

Mr. Chairman, I would yield the balance of my time to the ranking member, Mr. Jordan.

Mr. JORDAN. I thank the gentleman for yielding.

So we have got 50 million cameras in the country, a system that, as we said earlier, is—makes mistakes all the time. Those mistakes disproportionately hurt people of color. Violates First Amendment—I think violates First Amendment liberties, Fourth Amendment liberties, due process standards.

No elected officials are weighing in on this so that is sort of the list. But then I also think there is this chilling impact, this intimidation concept that is out there, and it seems to me this is in some ways—maybe I will give this question to you, Professor.

NAACP v. Alabama where, you know, disclosure—because this is going to be, like, constant disclosure. That, to me, as a lawyer, law professor, am I reaching or is there similarities to the whole intimidation that takes place when disclosure happens and this is going to be, in effect, a constant disclosure of what the heck you are up to?

Mr. FERGUSON. I think there is nothing more American than the freedom of expression and the freedom of association, and I think what we have seen is that this kind of technology can chill both of those—the ability to go out and protest in Baltimore or anywhere else, the ability to support an incumbent—you know, a political candidate who wants to go against—I mean, an upstart political candidate who wants to go against the incumbent.

It is going to chill speech. It is going to chill association and we are not going to be able to act in ways that we used to be able to act with anonymity.

Mr. JORDAN. Would you say it is—would you say it is just as bad as when the state wanted to require this organization to disclose its members for intimidation reasons? We all know that was the case. That this is, in effect, the same darn thing?

Mr. FERGUSON. It is the same First Amendment problem, yes.

Mr. JORDAN. Ms. Guliani, do you agree?

Ms. GULIANI. Yes. I mean, I think that one of the fundamental concerns that we need to address is I don't think any of us want to live in a world where there is a camera on every street corner that says, you know, who you are and maybe your emotional state,

right, and how do we prevent that surveillance buildup so that it doesn't look like some of the uses in China.

And whatever, I think, framework is put in place if there is a framework put in place I think needs to address those very real concerns.

And from my opinion, we don't have the solutions and we shouldn't be using the technology until we can be assured that people's rights can be protected.

Mr. JORDAN. Yes. Let us—let us at least have a debate with people who were actually elected versus unelected people just deciding.

Again, Mr. Chairman, I just want to say thank you. I got to run to something else here. But I want to thank our panel and I want to thank you again for this hearing. We do need to do something and I would say sooner rather than later.

Mr. MEADOWS. Will the gentleman yield?

Mr. JORDAN. Be happy to yield to my colleague.

Mr. MEADOWS. So because I am going to run to the same meeting, let me just tell you, you have now hit the sweet spot that brings progressives and conservatives together, and I—and, you know, and when you have a diverse group on this committee as diverse as you might see on the polar ends, I am here to tell you we are serious about this and let us get together and work on legislation.

And it is—the time is now before it gets out of control, and I yield back.

I thank the chairman.

Chairman CUMMINGS. Thank you very much, and we are—I think that we can get something done in a bipartisan way. That is music to my ears and I think it is a very serious issue. Thank you very much.

Mr. Connolly for a consent request?

Mr. CONNOLLY. Thank you, Mr. Chairman.

I would ask unanimous consent that the prepared testimony of the Information Technology and Innovation Foundation be entered into the record.

Chairman CUMMINGS. Thank you very much.

Mr. Welch?

Mr. WELCH. Thank you, and I want to thank the witnesses.

You know, oftentimes when there is a technology, as you pointed out, it will be used. However, the users see it to advance whatever their cause is, without any public input or any public limitations.

And you have been doing the hard work while Congress has really not been paying much attention. So I just want to say thank you for the important work that you have done.

Ms. Buolamwini—I am sorry—it was great to be with you at the conference on this at MIT and I see another conference member there as well.

We have heard a lot of disturbing examples about mass data collection. I just want to—and I think your idea of a moratorium makes a lot of sense.

And your view, as I understand it, is there ought to be affirmative consent, and how would that curb the effects of machine bias in the use of facial recognition?

Ms. BUOLAMWINI. So I believe there should be affirmative consent, meaningful transparency, and continuous oversight. Affirmative consent needs to happen because oftentimes these technologies are being used without our knowledge.

The example of Higher View came up because we have algorithmic bias in the wild stories where people will say, I didn't even know this technology was being used.

Affirmative consent matters when you are thinking about a case like what is happening with the tenants in Brooklyn where face recognition entry system is being installed against their will but at least you have public defenders who are coming up against them.

So regardless of the bias or how well the technology works, there should be a choice. But second, we need to know how well the technology works and what my research has shown is that the standards from the National Institute for Standards and Technology aren't even reflective of the American people.

So we have to start there to make sure that we even have a baseline for what is going on, and then there is continuous oversight because regardless of the accuracy, regardless of if there is consent, these systems, as the fellow panelists have mentioned, can be abused in all kinds of ways.

Mr. WELCH. Thank you. Thank you very much.

And Ms. Garvie, in your report "Garbage In, Garbage Out" you cite an example where the NYPD, when looking for a suspect who stole from a local CVS, was unable to find matches and they used the celebrity Woody Harrelson as an effort to get the identification, how is this problematic use of facial recognition technology allowed to happen? Essentially, because there are no rules now?

Ms. GARVIE. It is allowed to happen because there are no rules and there is no transparency either to the public to decide whether this is an appropriate use of a technology or not but also to defense attorneys and to the court to say is this producing reliable evidence.

It is not producing reliable evidence. But defendants aren't able to challenge it in court.

Mr. WELCH. And you also discussed the use of police sketches of, quote, "art" so there will be an artist's rendering of who they think it might be or—and how does that work with respect to protecting defendants?

Ms. GARVIE. That is right. So forensic sketches are submitted to face recognition systems in at least six jurisdictions around the country.

This is, roughly, the equivalent of—well, face recognition is considered a biometric identification tool. Imagine if we had a fingerprint lab drawing fingerprints or drawing where a latent print's fingers—finger ridges ended with a pen, submitting that to search. That would be a scandal. That would e reasons for a mistrial or for convictions being overturned. So it is hugely problematic.

Mr. WELCH. Okay. Thank you. Thank you.

Ms. Buolamwini, again, if the technology improves so that that the racial bias was, quote, "eliminated," not that necessarily it will ever happen, would you still recommend mandating affirmative consent?

Ms. BUOLAMWINI. Even if you improve the racial biases, for example, there is a case reported by the intercept where IBM equipped the New York Police Department with video capabilities to search people by their skin type, by their facial hair, by the clothing that they were wearing.

So you could also automate the tools for racial surveillance and racial profiling even if you made these accuracy disparities go away, which right now the statistical evidence does not support. So yes, you would still need consent in the use of these technologies.

Mr. WELCH. Thank you very much.

Mr. Chairman, I yield back.

Chairman CUMMINGS. Thank you very much.

Ms. Kelly?

Ms. KELLY. Thank you, Mr. Chairman, for holding this hearing today on facial recognition technology.

Last Congress, the IT Subcommittee held a series of hearings on artificial intelligence and in the white paper that I wrote with Rep. Will Hurd we discussed the issues of bias and the importance of algorithmic accountability and transparency.

As facial recognition is used more in society, it is vital that this technology not perpetuate real-world biases that harm minority communities. Say your name for me because I want to make sure I say it right.

Ms. BUOLAMWINI. Buolamwini.

Ms. KELLY. Ms. Buolamwini. Okay. What are some of the benefits that racial—that facial recognition technology can provide?

Ms. BUOLAMWINI. So one area that has been explored right now is the use of facial analysis technology in health care—could we be able to maybe spot, let us say, something like a stroke or heart disease—other things that might be actually perceptive from the face.

So that is the promise, and oftentimes what I see is the promise of this technology is not met by the reality. You have new research coming out from the University of Toronto that shows even for health care-based systems of facial analysis technology you are starting to see biases.

So you get a bias when it comes to accuracy when you are looking at age or somebody has dementia versus not. So I am hopeful that research can continue to explore potential uses. But until we have shown that it actually meets the promise, it should not be used.

Ms. KELLY. In your testimony you discuss the lack of mandated accuracy requirements that test the maturity of facial recognition technology. How do you believe this test should be conducted and who should approve the technologies as adequately mature?

Ms. BUOLAMWINI. Absolutely. Well, one thing that we have to acknowledge is when we are looking at facial analysis technologies, one metric—accuracy—isn't enough. Not only do we want to know how accurate a system might be but we want to know how it fails, right. Who are the false positives? Who are the false negatives?

Right now in the U.S. we have the National Institute for Standards and Technology, which does mandate tests. There are voluntary tests around facial analysis technology. So that could be one agency that is employed to figure out what are the necessary metrics that could come in place.

What we are seeing right now is the way that the systems are tested are very limited. So when I mentioned pale male data sets earlier on, we can actually have a false sense of progress if the evaluation standards that are meant to be the gold standards don't even represent everybody right now.

So we need to change the way in which we evaluate facial analysis technology so we truly understand who it works for and who it fails on.

Ms. KELLY. I am not sure how much time I have because—Okay, now it is corrected, I guess.

But should the use case dictate the level of maturity and should the government and private industry have different standards?

Ms. BUOLAMWINI. I definitely believe the use case matters. If you are using facial analysis to animate an emoji or to put on SnapChat filters that is a different case than if you are saying we are going to use facial analysis to infer your emotional engagement or problem solving ability to inform a hiring decision, which is what we are seeing with products coming out of Higher View. So the use case absolutely matters.

Ms. KELLY. Ms. Garvie, you mentioned an EEF study where the authors recommended facial recognition and in quotes "only be used to identify individuals already detained by law enforcement and under policies restricting its use in specific instances of criminal conduct."

Do you believe that this use would be an appropriate use of the technology for use today and are there any other safeguards that you would like to see implemented?

Ms. GARVIE. I do. Oh.

Ms. KELLY. Also, before you answer that—I am getting my question—you and Dr. Alexander, as we talk about having legislation, who do you think should be at the table?

Of course, we should be at the table but who else should be at the table? Because we are not the experts, so as we come up with rules and regulations.

Ms. GARVIE. I fundamentally believe it is up to communities to decide to take a close look at how this technology is being used, what its capabilities and limitations are and decide whether the risks outweigh the benefits.

San Francisco has taken that look and decided that the risks do not outweigh those benefits. In my personal view, I think some communities will come out differently, will say that there are instances, probable cause where law enforcement needs to know who is in custody.

Fingerprinting has failed. That may be an appropriate use for this technology. But fundamentally, that needs to be a decision made by legislatures, not by law enforcement agencies.

Mr. ALEXANDER. Yes, ma'am.

Yes, ma'am. I certainly do think a couple of things. One here is that certainly you need to be at the table. The technology developer of that software needs to be at the table. Public safety needs to be at that table.

ACLU needs to be at that table, and other legal persons as well, too, so that if we are going to utilize this technology in public safety, in law enforcement, I think one thing needs to be made clear

to these software manufacturers is that if you are going to develop this technology it is going to have to meet a standard that you hear being articulated at these—at this table by the scientists and those in the legal communities that are here.

It needs to meet that standard. If it can't meet that standard, then there is no place for it in our society. Police need to be at the table so they can clearly understand if you decide—your jurisdiction decide to pay for and acquire this technology, you are going to be held to a standard as well, too.

Not just training, but the way in which you apply it, how it is applied, and you are going to be held responsible as a public safety agency to sharing in your local community how this technology was developed, why it was developed, and the use of it, and also where it may not be as effective as we think.

Because this is a huge—this is a huge, very complicated convoluted piece of technology that may have some benefits that you have just heard but they also have a significant amount of challenges attached to them.

Ms. KELLY. And are there a amount of hours that police departments or law enforcement are trained right now or is it just hit or miss?

Mr. ALEXANDER. You know, I can't say that specifically. But my sense it is kind of hit or miss because we know that there are agencies out there right now and I have the persons here at this table who can certainly attest to that, that this technology is introduced into those departments and there is very little training and certainly no policy development around it.

And then when you ask those in those agencies, tell me about the technology and how it work, they can't do it and that is a real problem.

Ms. KELLY. Thank you. I yield back.

Chairman CUMMINGS. You know, it is a—before I got to Ms. Miller, it is a shame, Dr. Alexander, the whole thought of people being arrested and losing their jobs and everything based on errors.

Mr. ALEXANDER. Right.

Chairman CUMMINGS. And that is a problem. One of the things that I question, too, is John Lewis—Congressman Lewis and I——

Mr. ALEXANDER. Yes, sir.

Chairman CUMMINGS [continuing]. are mistaken for each other. If I go out there right now, I guarantee you there will be at least five or six people that will call me John Lewis. And I have actually had him in my district where I live and they call him me. That is a problem. I mean, I am glad it was John Lewis—a good name.

Ms. Miller?

Ms. MILLER. Thank you, Chairman Cummings and Ranking Member Comer, and to all of you all for being here today.

As technology continues to evolve and grow, the question of proper uses for facial recognition in our society is becoming increasingly important.

Ms. Garvie, how far out are we in the United States from having facial recognition technology that is 100 percent accurate on photos of people in all demographics?

Ms. GARVIE. I don't—I can't speak to the—where the technology is at. But I will say based on how law enforcement agencies use

the technology it doesn't matter how good these algorithms get if low-quality images or the images of wrong people are submitted, which is what we are seeing at the law enforcement level.

Ms. MILLER. Are there any cities in the United States that are deploying real-time face surveillance?

Ms. GARVIE. We see Chicago and Detroit have both acquired the technology. We do not know the level to which it has been deployed.

In 2013, Chicago did report back to the DHS, the funder of their system, that the capabilities were up and running. They have since said they do not use the capability. We don't know about Detroit.

A handful of other agencies across the country—Los Angeles, the West Virginia Intelligence Fusion Center, and others—have either piloted or have looked to purchase this technology as well.

Ms. MILLER. Okay. Are there any Federal agencies, to your knowledge, that utilize real-time face surveillance?

Ms. GARVIE. The U.S. Secret Service is piloting a program around the White House complex as we speak. We do not know the degree to which the FBI has been piloting this. We do know they have acquired or have been using Amazon recognition, which is the same surveillance capability that Orlando has been piloting in real time. But there is no transparency into how and when they are using that.

Ms. MILLER. All right. To you and Ms. Guliani, can you discuss some of the wrongful arrest cases that have arisen as a result of the inaccuracy for the facial recognition?

Ms. GULIANI. Sure. I think that one of the concerns is that we don't even have a handle on the full scope of cases and that is because, No. 1, we are not seeing data about how often these algorithms are resulting in false matches, and No. 2, when defendants are being charged they are not necessarily being provided notice or given all the information.

So the question you ask is a very good one but it is one that we don't actually have I think full data about.

Ms. GARVIE. I would echo that. I speak to public defenders a lot. There have been close to 3,000 arrests in New York made including the use of face recognition technology.

Those 3,000 defendants were not told that face recognition was used. Maybe some of them were. A vast majority of them were not.

Ms. MILLER. Well, like Chairman Cummings, I have had many people tell me that they have seen my twin somewhere else and I think we all resemble someone else. So it is kind of scary.

Have there been—can you see—can you set a Federal floor for minimum standards for the use of facial recognition technology and what would those Federal standards look like? Both of you.

Ms. GULIANI. I think that when we are having this conversation one of the questions we should be asking is, is there an alternative that is less invasive, right.

We have talked about how face recognition is different and how it raises fundamental concerns with regards to our First Amendment rights, with regards to persistent and constant tracking.

There are very real risks with this technology and we should be asking are there other alternatives that can serve the same needs that are less invasive and less concerning, and I think that that

would be helpful to have as we are having this debate to determine what the standard should be and whether there are uses, if any, that should be permitted.

Ms. GARVIE. I would agree, and I think the constitutional risks that face recognition pose provide good guidance for a legislative floor—prohibitions on use that would violate the Fourth Amendment that would risk chilling free speech, that would affect the Fourteenth Amendment rights to due process and equal protection.

Ms. MILLER. That was my next question. So thank you.

I yield back my time.

Chairman CUMMINGS. Ms. Ocasio-Cortez?

Ms. OCASIO-CORTEZ. Thank you, Mr. Chair.

Ms. Buolamwini, right now Amazon can scan your face without your consent—all of our faces without our consent—and sell it to the government, all without our knowledge, correct?

Ms. BUOLAMWINI. Yes.

Ms. OCASIO-CORTEZ. And, you know, Mr. Chair, I would like to seek unanimous consent on how Amazon actually met with ICE officials over a facial recognition system that could identify immigrants. I would like to submit this to the congressional record.

Chairman CUMMINGS. Without objection.

Ms. OCASIO-CORTEZ. Thank you so much.

Ms. Garvie, in fact, it is not just Amazon that is doing this, right. It is Facebook. It is Microsoft. It is a very large amount of tech corporations, correct?

Ms. GARVIE. That is correct.

Ms. OCASIO-CORTEZ. And do you think it is fair to say that Americans are essentially being spied on and surveilled on a massive scale without their consent or knowledge?

Ms. GARVIE. I would make a bit of a distinction between what Facebook and other companies are doing but yielding to Ms. Buolamwini for more specifics on this. I will say most of the law enforcement agency systems operate on DMV data bases or mug shot data bases. So information that has been collected by agencies rather than companies.

Ms. OCASIO-CORTEZ. Great. Thank you. Thank you.

And Mr. Ferguson, one the prime constitutional concerns about the nonconsensual use of facial recognition technology is rooted or alluded to in the Fourteenth Amendment, correct?

Mr. FERGUSON. That is correct. It is one of them.

Ms. OCASIO-CORTEZ. And right now companies, governments, agencies can essentially steal or use your biometric data from you without your consent and this is outrageous, right, because this is America and we have a right to privacy. Isn't that right, Ms. Guliani?

Ms. GULIANI. That is absolutely right.

Ms. OCASIO-CORTEZ. And Ms. Guliani, what was the Supreme Court case that identified the right to privacy?

Ms. GULIANI. It has been—I don't remember the original one. But, I mean, there has been a series of cases where the court has essentially said, look, with modern technology it shouldn't mean that we don't have Fourth Amendment rights.

Ms. OCASIO-CORTEZ. Yes. And what was—was there a landmark Supreme Court decision that established that that we have seen recently?

Ms. GULIANI. You know, we have seen the Carpenter case where the court said that it was unconstitutionally—unconstitutional to warrantlessly surveile individuals.

We have seen cases where the court has also said that you can't search a cell phone without a warrant leading to an arrest.

Ms. OCASIO-CORTEZ. And most specifically, with relation to the Fourteenth Amendment, it was Roe v. Wade that established the right to privacy. Is that correct?

Ms. GULIANI. Roe v. Wade—the right to privacy was addressed there as well.

Ms. OCASIO-CORTEZ. Right. So, you know, we don't just have—because that right to privacy is alluded to. Part of the case in our right to privacy is that this doesn't just give us a right to my uterus.

It gives me a right to my hand and my shoulders, my head, my knees, my toes, and my face. And so in some ways, part of the case, although it is not all of it—there is a great deal rooted in the Fourteenth Amendment with search and seizure—but in our right to privacy we also see here that it is—this is about our entire body—our right to our entire body and the similar principle that keeps a legislator out of my womb is the same principle that would keep Facebook and algorithms off of all of our faces. And so do you think there is a—it is fair to draw that connection?

Ms. GULIANI. I think that when we are talking about privacy it is important to think about more than our face, right. So we are seeing the FBI use things like voice recognition and gait recognition, all different types of biometrics that I think fundamentally raise some of the same privacy concerns that have been talked about by all the panelists today.

Ms. OCASIO-CORTEZ. Thank you. Thank you so much.

And Ms. Buolamwini, I heard your opening statement and we saw that these algorithms are effective to different degrees. So are they most effective on women?

Ms. BUOLAMWINI. No.

Ms. OCASIO-CORTEZ. Are they most effective on people of color?

Ms. BUOLAMWINI. Absolutely not.

Ms. OCASIO-CORTEZ. Are they most effective on people of different gender expressions?

Ms. BUOLAMWINI. No. In fact, they exclude them.

Ms. OCASIO-CORTEZ. So what demographic is it mostly effective on?

Ms. BUOLAMWINI. White men.

Ms. OCASIO-CORTEZ. And who are the primary engineers and designers of these algorithms?

Ms. BUOLAMWINI. Definitely white men.

Ms. OCASIO-CORTEZ. So we have a technology that was created and designed by one demographic that is only mostly effective on that one demographic and they are trying to sell it and impose it on the entirety of the country?

Ms. BUOLAMWINI. So we have the pale male data sets being used as something that is universal when that isn't actually the case when it comes to representing the full sepia of humanity.

Ms. OCASIO-CORTEZ. And do you think that this could exacerbate the already egregious inequalities in our criminal justice system?

Ms. BUOLAMWINI. It already is.

Ms. OCASIO-CORTEZ. Thank you very much. I yield the rest of my time to the chair.

Chairman CUMMINGS. How so?

Ms. BUOLAMWINI. So right now, because you have the propensity for these systems to misidentify black individuals or brown communities more often and you also have confirmation bias where if I have been said to be a criminal that I am more targeted, so there is a case with Mr. Bah, an 18-year-old African-American man, who was misidentified in Apple stores as a thief and in fact he was—he was falsely arrested multiple times because of this kind of misidentification.

And then if you have a case where we are thinking of putting let us say facial recognition technology on police body cams in a situation where you already have racial bias that can be used to confirm, right, the presumption of guilt even if that hasn't necessarily been proven because you have these algorithms that we already have sufficient information showing fail more on communities of color.

Chairman CUMMINGS. Mr. Grothman?

Mr. GROTHMAN. Okay. I guess this is probably for Ms. Garvie but it could be really for anybody.

China makes a lot of use of this technology, correct?

Ms. GARVIE. Yes.

Mr. GROTHMAN. Could you let me know the degree to which it exists in China? And I believe they even kind of brag about selling this technology to other countries?

Ms. GARVIE. We probably don't know the full degree to which it is used. We do see face surveillance capabilities where the government is attempting to enroll all faces of all citizens into their data bases to be able to effectively identify where anybody is at a given time in addition to classify people by the characteristics of their face to try to be able to identify who is a Uyghur Muslim minority.

Mr. GROTHMAN. Okay. And I could tell Mr. Ferguson wanted to jump in there. Are they trying to sell this technology to other countries?

Mr. FERGUSON. Yes.

Mr. GROTHMAN. And for what purpose? When they go into—I am not sure which other countries they are selling it to, but when they go into another country, what are the benefits that they describe this technology as being used for?

Mr. FERGUSON. China has created a truly—a true surveillance state where they are able to use hundreds of millions of cameras and artificial intelligence matching of face recognition to identify people on the streets.

And so for certain authoritarian governments that is very attractive there.

Mr. GROTHMAN. And why is it attractive?

Mr. FERGUSON. I think because it is a form of social control. One of the things that they have been doing is they have rolled it out to prevent jaywalking. So that one of the ways they do it is to say as people walk past the camera you will be shamed because you were a jaywalker.

Mr. GROTHMAN. Well, not just jaywalking. As I understand it, it is also used to monitor how people think or people who may think one way or another. Is that true?

Mr. FERGUSON. It is being used to surveile religious minorities and dissenting opinions and thus controlling the way they think and the way they react. And so that is, obviously, there are lots of human rights abuses that we have seen coming out of China.

Mr. GROTHMAN. Okay. So in other words, monitor the Muslims, and I can't remember what they call that group.

Mr. FERGUSON. The Uyghurs, yes.

Mr. GROTHMAN. Uyghurs. Uyghurs on the western end, and Christians——

Mr. FERGUSON. Yes.

Mr. GROTHMAN [continuing]. throughout the country. So we place them so that if there is a church that we know about we know exactly all who is going in there, and they sell this as a—I think they describe it as kind of—they have reached the perfect government.

They have got a free market in the economy so it is a wealthy society but they have complete control about how people think and behave otherwise or do what they can to control it. Is that right?

Mr. FERGUSON. That is right, and the scariest thing is that technology could be rolled out on the streets of Washington, DC. tomorrow because there is no law saying that it couldn't be, and that is what we need to address.

Mr. GROTHMAN. Do you happen to know—I mean, I have read that they have tried to sell this—almost sell a form of government, but this is a big part of that form of government—to other countries.

Do you know any other countries specifically who are biting at this opportunity or is it just something they are starting out doing?

Mr. FERGUSON. I don't know as a political matter. I know as a technological matter this is a multi-billion dollar industry of cameras and algorithms and there is tremendous investment by the Chinese government in improving it.

Mr. GROTHMAN. Do you know any other countries they have—have had success at selling this to?

Ms. BUOLAMWINI. So there is an example where you have a Chinese company called Cloud Walk that provide the government of Zimbabwe with surveillance technology and this enables them to have access to darker-skinned individuals. So you are starting to also see the emergence of what is being called data colonialism.

Mr. GROTHMAN. Okay. So in other words, they are telling Zimbabwe that they can do what China does. They can monitor who is here, who is there and——

Ms. BUOLAMWINI. But in exchange for something very valuable, which would be the dark-skinned faces to train their system so that they can then sell it, let us say, to the U.S. where you have dark-skinned individuals as well.

Mr. GROTHMAN. Well, I—as I understand it, though, the clear goal of a government using these, if, you know, as America becomes more intolerant, as we have micro-aggressions, as we, you know, begin to have politically incorrect gathering places—a gun show or something—is it something that we should fear that our government will use it to identify people who have ideas that are not politically correct?

Ms. GARVIE. Law enforcement agencies themselves have expressed this concern. Back in 2011 when the technology was really getting moving, a face recognition working group including the FBI said—and they said exactly that face recognition could be used as a form of social control, causing people to alter their behavior in public, leading to self-censorship and inhibition. So this is something police departments themselves have recognized.

Mr. GROTHMAN. Thank you for having a hearing on this topic. It is very important.

Chairman CUMMINGS. Ms. Pressley?

Thank you.

Ms. PRESSLEY. Thank you, Mr. Chairman.

Last week, San Francisco became the first city to ban use of facial recognition technology. But a similar ban is being considered in my district, the Massachusetts 7th congressional District, by Somerville, Massachusetts, and it is the first on the East Coast to propose such a ban.

Facial recognition technology has been used by law enforcement in Massachusetts since 2006 but there are concerns about due process, given the police and prosecutors do not notify defendants when the technology has been used in their cases.

I do believe the Federal agencies should not use this technology without legislative authorization and these due process violations are a perfect example as to why.

But companies have been pushing this technology on police departments, despite knowing that it works only 30 percent of the time. This puts many people, including women and people of color and young people, at grave risk of harm and underscores the need for congressional oversight.

Ms. Buolamwini, first, I want to say I am so proud that AJL is in the Massachusetts 7th. You are based in Cambridge, correct?

Ms. BUOLAMWINI. We are.

Ms. PRESSLEY. So I am so glad that you call the Massachusetts 7th your home. In a New York Times article from June of last year titled, "When the Robot Doesn't See Dark Skin," you describe how and why these inaccuracies exist. You refer to the, and I quote, "coded" gaze. Can you describe this phenomenon, for the record?

Ms. BUOLAMWINI. Sure. So you might have heard of the white gaze or you might have heard of, let us say, the male gaze, and these descriptions are descriptions of power—who has the power to decide.

And so when I talk about the coded gaze I am invoking the male gaze and the white gaze and it is a question of whose priorities, preferences, and also prejudices are shaping the technology that we are seeing.

So right now, the way I look at AI is we see this growing coded gaze that is mainly pale, mainly male, and doesn't represent the majority of society.

Ms. PRESSLEY. Thank you.

Ms. Garvie, in your Georgetown report you found that, and I quote, "There is no independent testing regime for racially biased error rates," unquote. Is this still the case today?

Ms. GARVIE. NIST has since then adopted looking at the differential error rates between race and gender in their studies. They have yet to look at the inter-sexual intersectional consequences of that. But they are starting to take a look.

Ms. PRESSLEY. Okay.

And Ms. Buolamwini, are there any measures developers of this technology can take right now to increase the accuracy of their facial recognition systems?

Ms. BUOLAMWINI. Right now what we have seen in the research studies that have happened thus far to improve these systems tends to be around the kind of data that is used to train the systems in the first place.

But we have to be really cautious because even if you make accurate facial analysis systems they can and will be abused without regulations.

Ms. PRESSLEY. All right. Very good.

Ms. Guliani, in your testimony you raise the example of Willie Lynch who claims to have key details about the reliability of a facial recognition algorithm that led to his arrest and conviction.

In his case it was a low confidence match of a poor quality photo. Can you talk about the challenges that individuals may take rebutting a face recognition match and how is it different than eyewitness identifications?

Ms. GULIANI. Sure. I mean, with an eyewitness you can put that person on the stand. You may raise questions about how good their eyesight is, how far away they are, whether they were intoxicated at the time they made that identification.

It is quite different with face recognition. I think people are assuming that it is 100 percent accurate, and fundamentally a lot of individuals are not able to get information about the reliability of the algorithm.

In the case you just referenced, that is still an ongoing case where Willie Lynch is fighting to get information about an algorithm that could be used to challenge his conviction.

Ms. PRESSLEY. Do you believe the FBI or other law enforcement agencies have adopted sufficient safeguards to prevent its face recognition technology from resulting in these civil rights abuses?

Ms. GULIANI. Absolutely not, and I certainly think this is an area where additional oversight is needed. When the FBI rolled out the system, they made a lot of promises.

They made promises about accuracy. They made promises about testing. They made promises about protecting First Amendment rights. And now, years later, a lot of those promises have been broken.

The agency has not acknowledged a responsibility to test the accuracy of systems it uses of external partners. There is questions about how accurate their systems are, and it doesn't appear that

they have a high standard in place for when they are running face recognition searches.

And I think all of those things are cause for concern and should really cause us to question whether the system should still be operating, given the lack of safeguards.

Ms. PRESSLEY. Thank you. I yield back.

Chairman CUMMINGS. Thank you very much.

Mr. Amash?

Mr. AMASH. Yes, thank you, Mr. Chairman.

The Supreme Court recognized recently that a person does not surrender all Fourth Amendment protection by venturing into the public sphere. Face recognition surveillance threatens to shatter the expectation Americans have that the government cannot monitor and track our movements without individualized suspicion and a warrant.

It is difficult to comprehend the impact such surveillance would have on our lives. With face recognition technology deployed throughout a city, anyone with access to the data could track an individual's associations and public activities, including religious, political, medical, or recreational activities.

Ms. Garvie and Ms. Guliani, could a government's access to this kind of data have a chilling effect on First Amendment activities and other constitutional activities and rights such as gun ownership, the free exercise of religion, the freedoms of speech and of the press and the right of the people peaceably to assemble and petition the government, and how could data gathered from face recognition surveillance be weaponized by the government against activities protected by the Constitution?

Ms. GARVIE. To your first question, absolutely. Yes. And this is something that law enforcement agencies themselves have acknowledged.

In terms of how this can be used, the mere threat or fear of monitoring or identifying every single person at a protest or a rally, particularly around contentious or highly disputed concepts, could cause people to stay at home, to not have those conversations, to not engage in those discussions that are so valuable for the participation in an active democracy.

Ms. GULIANI. And we have seen examples where there have been requests for face recognition without cause. So in Vermont there was a case where there was request for a face recognition match even though the individual was not suspected of a crime. They were just the girlfriend of a fugitive.

There was another case where the basis of the request was simply that someone had asked concerning questions at a gun store without any allegation that they had actually committed a crime.

And so I think that speaks to the concern you are talking about, which is we don't want to live in a world where we can be identified without our knowledge secretly and on a massive scale, which is exactly what face recognition allows.

Mr. AMASH. Ms. Garvie and Professor Ferguson, even if we require law enforcement to get a warrant to run a search on face recognition data from surveillance cameras, would it be possible for such cameras to use face recognition technology in public areas

without effectively gathering or discovering information on innocent people who are not the subject of an investigation?

Ms. GARVIE. No. That is not the way the face recognition systems work. Unfortunately, in order to identify the face of the person you are looking for you have to scan every single face of everybody else who you are not looking for.

Mr. FERGUSON. That is correct, and I think that the problem—even a probable cause standard may not be enough and you have to take steps to minimize if you are going to do this for particular reasons, which is why a probable cause plus or something higher should be part of Federal legislation on this.

Mr. AMASH. Thanks. Ms. Garvie and Ms. Guliani, what dangers could access to this data pose to the rule of law and to keeping our government free of corruption?

Could abuse of face recognition data give officials the ability to influence political or business decisions or to unfairly target or benefit from such decisions? Does face recognition surveillance data need any increased protections to make sure these kinds of abuses don't occur?

Ms. GULIANI. The risk of abuse is substantial and the reason there is that risk of abuse is, No. 1, this technology is very cheap. You can run thousands of searches for just a handful of dollars. Two, it is being done secretly, right, so individuals don't necessarily know and can't raise concerns.

And three, it is being done on a massive scale. I mean, we talked about access to driver's license photos and the extent to which it affects everybody in those data bases.

We are going to—getting to a point where, you know, virtually everybody is in a face recognition data base, which gives the government enormous power. And so I think we need to think about those concerns before moving forward with this technology.

Ms. GARVIE. Think of a way that identifying somebody just because they show up in public in the—you know, with a camera present could be used and chances are it can and will be used in the absence of rules.

Mr. AMASH. All right. Thanks. I yield back.

Chairman CUMMINGS. Thank you very much.

Mr. Gomez?

Mr. GOMEZ. Thank you, Mr. Chairman.

I want people to imagine that they are driving home from work and then they see in the rear view mirror, you know, red and blue lights. They have no idea why the police are behind them.

You know, they weren't speeding. They didn't run a stop sign. But you know what? They pull over like everybody should. A voice over a loudspeaker commands them to exit their vehicle and as you do you see seven police officers, guns drawn, and they are pointing right at you. One wrong move, a mistake, a misunderstanding, a miscommunication can mean the difference between life and death.

That is what is called a felony stop, one of the most common high-risk situations police find themselves in, and it all started earlier in the day when a police officer ran a search with a—through a facial recognition data base and it incorrectly identified you as a violent felon, and you had no idea that that even occurred.

That is just one of the scenarios that I think about when it comes to this technology—one of the many things that could possibly go wrong.

I must admit, I was not even paying attention to this technology until I was misidentified last year during the ACLU test of Members of Congress and it really did spark an interest and a curiosity of this technology and really did feel wrong deep in my gut that there is something wrong with this technology.

I started looking into it since last year. I have had nine meetings. My office has had nine meetings with representatives from Amazon. We have asked questions from experts across the spectrum, and my concerns only grow day by day.

Until February of this year, Amazon had not submitted its controversial facial recognition technology recognition to third party testing with the National Institute of Standards and Technology, known as NIST.

In a January 2019 blog post, Amazon stated that, quote, "Amazon recognition can't be downloaded for testing outside of Amazon." In short, Amazon would not submit to outside testing of their algorithm.

Despite the fact that Amazon had not submitted its facial recognition product to outside testing, it still sold that product to police departments.

In 2017, police in Washington County, Oregon, started using Amazon recognition technology.

Ms. Buolamwini——

Ms. BUOLAMWINI. Buolamwini.

Mr. GOMEZ. Buolamwini. Do you think that third party testing is an important safe deployment—is important for safe deployment of facial recognition technology?

Ms. BUOLAMWINI. Absolutely. One of the things we have been doing at the Algorithmic Justice League is actually testing these companies where we can, and this is only—we are only able to do the test for the output. So we don't know how these companies are training the systems. We don't know the processes in place when they are selling the systems.

All we know is when we test on our more comprehensive or more inclusive data sets what are the outcomes. So we absolutely need third party testing and we also need to make sure that the National Institute for Standards and Technology—NIST—that their tests are comprehensive enough.

Our own research show that some of the benchmarks from this were 75 percent male, 80 percent lighter skinned. So even when we have companies like Microsoft who figured out how to let NIST test their system, unlike Amazon, was claiming they couldn't, even when we have those performance results we have to see what data set it is being evaluated on.

Mr. GOMEZ. Yes, correct. Because if it is evaluated on a data set that is incorrect or biased it is going to lead to incorrect results, correct?

Ms. BUOLAMWINI. Or an incorrect false understanding of progress. So back in 2014, Facebook released a paper called "DeepFace" and they reported 97 percent accuracy on the gold standard benchmark at the time.

But when you looked at that gold standard benchmark it was 77 percent male and around 80 percent white individuals. And so as a result—or over 80 percent. So you don't know how well it actually does on the people who are not as well represented.

Mr. GOMEZ. Before I run out of time, what organizations are equipped to accurately test new facial recognition technologies?

Ms. BUOLAMWINI. The National Institute of Standards and Technology is currently doing ongoing testing. But they need to be better.

Mr. GOMEZ. Okay. Now, I appreciate it. This is a major concern. I think that you are seeing the—both parties and across the ideological spectrum showing some reservations about the use of this technology.

I am glad to see the chairman of this committee look at this issue and I look forward to the next hearings that we will be having.

Mr. Chairman, with that I yield back.

Chairman CUMMINGS. Yes. Mr. Gomez, I do expect that we are going to be able to get some legislation out on this. I talked to the ranking member. There is a lot of agreement. The question is do you have an all-out moratorium and at the same time try to see how this process can be perfected.

But, clearly, you are absolutely right. There is a lot of agreement here, thank God.

Ms. Tlaib?

Ms. TLAIB. Thank you, Chairman.

With little to no input, the city of Detroit created one of the Nation's most pervasive and sophisticated surveillance networks with real-time facial recognition technology.

Detroit's $1 million face-scanning system is now tracking our residents on hundreds of public and private cameras at local parks, schools, immigration centers, gas stations, churches, health centers, and apartment buildings.

My residents in the 13th congressional are burdened with challenges that most Americans couldn't bear themselves and laid on top of these economic challenges and structural racism that hurts our children more than anyone in the family is the fact that policing our communities has become more militarized and flawed.

Now we have for-profit companies pushing so-called technology that has never been tested in communities of color, let alone been studied enough to conclude that it makes our communities safer.

So Dr. Alexander, have you see police departments develop their own approval process concerning the use of facial recognition? If so, how are these policies determined?

Ms. GARVIE. It seems like Dr. Alexander stepped out, but I could take a stab at answering that question, if that would help.

Ms. TLAIB. Thank you.

Ms. GARVIE. So my research includes FOIAs to a couple hundred agencies. We have seen some agencies develop policies. Detroit does have a policy around their use of face recognition.

Concerningly, however, that policy states that their face surveillance system may be expanded beyond its current conception to drones and body cams as well.

So it is not uncommon to see policies saying there might be some restrictions on its use but also affirmatively encouraging the use of the technology or reserving the right to expand it far beyond existing current capabilities.

Ms. TLAIB. Ms. Garvie, right? Can you—do you know if these policies include any initial justification on the need for the facial recognition technology program, and second, in that policy for Detroit does it prevent them from sharing this data or information with any Federal or state agencies?

Ms. GARVIE. Most policies that I have read do not provide an initial justification beyond that it is a law enforcement investigative tool.

I would have to get back to you on the question about what Detroit's policy specifically says. I do not recall any language either prohibiting or allowing that. But I would have to get back to you.

Ms. TLAIB. Are we seeing any uniformity in these policies across law enforcement agencies at all?

Ms. GARVIE. No.

Ms. TLAIB. How are—have any of these policies proven to be effective? I think we all agree that there is too many flaws for it to be effective, correct?

Ms. GARVIE. Correct, and one of the problems is most of these policies are not available to the public. We have seen far more policies now, thanks to FOIA processes and FOIA litigation to try to get information.

But the LAPD, the NYPD, and other jurisdiction initially tell us they have no records, even though they may have records or they may have systems. So there is a fundamental lack of transparency around this as well.

Ms. TLAIB. Yes. Chairman, if I may submit for the record an article, "Researchers Alarmed by Detroit's Pervasive Examining Facial Recognition Surveillance Program," talking about the little to no input and transparency in the implementation of that program.

Chairman CUMMINGS. Without objection, so ordered.

Ms. TLAIB. In the response to this lack of kind of oversight we have heard various organizations advocate for independent police oversight board or judicial approval for the use of facial recognition technology on a case by case basis which would require a probable cause standard.

Professor Ferguson, can you speak about the benefits of this approval process?

Mr. FERGUSON. There would be some approval—some check if there was at least a probable cause standard. I think that with the danger of facial recognition it might even need to be higher than just probable cause, more of a probable cause plus kind of idea.

You would also take care of the minimization requirements. You would be certain of the data and what would happen to it. But at least it is some check.

Right now, this technology is being deployed without that check in most cases, and having Federal legislation, state legislation, and local legislation on it and a third party check of a judge would certainly be an improvement.

Ms. TLAIB. And, you know, I get this a lot. There are some that argue that probable cause plus warrant would be too burdensome

for law enforcement officials and would not allow them to move quickly when attempting to catch a potential criminal.

Do you agree with this assertion?

Mr. FERGUSON. No, I don't think it is that hard. If you have probable cause of a crime, you know you have an identification and you want to search a data base, I think a judge will sign off on it. Judges now can get warrants electronically on their iPads. I don't think it is that much of a burden anymore.

Ms. TLAIB. I couldn't agree more. A person's freedom is at stake.

So thank you so much. Thank you, Mr. Chairman. I yield the rest of my time.

Chairman CUMMINGS. Thank you very much.

Mr. Lynch?

Mr. LYNCH. Thank you, Mr. Chairman, and let me congratulate you on a very—just an excellent hearing and I want to thank the witnesses. You have done a tremendous service, I think, to this committee and I am sure that your thoughts and inputs will be reflected in some of the legislation that comes out of here.

For the record, I would like to ask unanimous consent to submit Massachusetts Senate Resolution 1385 and Massachusetts House Resolution 1538. This is the legislation that would put a moratorium on facial recognition in my state of Massachusetts.

Chairman CUMMINGS. Without objection.

Mr. LYNCH. Thank you.

And I don't usually do this, but I read this excellent book about a month ago. It is by Shoshana Zuboff over at Harvard, "Surveillance Capitalism," and it changes—it really changed the way I look at all of this.

I am actually the chairman of the Fin Tech Task Force here in Congress on the Financial Services Committee, and she did a wonderful job with the book.

And I believe that—after reading this that our focus today just on facial recognition and just on law enforcement's use of this information and just, you know, public surveillance is far too narrow.

You know, right now in this country we have about 257 million smart phones. About 100 million of those are iPhones. So because we click "I agree" when we use those apps, even though the average American spends about 14 seconds reading that agreement, and we click "I agree."

And so what we don't know is that when we click "I agree" it allows Apple, Google, Facebook to use, to share, to sell all of our information.

So, you know, they track what we look—not only what we look like but who our friends are or where we go each and every day, tracking our motion, every selfie we take that gets uploaded, every book we have read, every movie we see—you know, how we drive. AllState now has an app where you—you know, if you let them track you and you don't drive crazy they will lower your rates, you know, so there is this—so right now, you know.

And the Internet of Things—my coffee maker and my toaster is hooked up to the internet. You know, I am not sure I really need that. But my vacuum cleaner, although I don't use it very often, is hooked up to the Internet of Things.

So what we have right now—my iWatch. You know, I am a victim here. I have got everything going. But——

[Laughter.]

Mr. LYNCH. The problem is we have total surveillance and we are looking at this one little piece of it—you know, facial recognition—and I worry that we are missing all of—all of the other—the dangers here just because it is not the government. It is Facebook. It is Google. It is Microsoft. It is Apple.

And to go back to Mr. Grothman's point a while ago, OPM, you know, gathered up all of our information here in Congress and then they were hacked. They didn't encrypt any of our Social Security numbers or anything. So we believe it was the Chinese. They got all that information.

And so now we are allowing Apple, Google, Facebook to maintain these huge and granular descriptions of who we are, and they have been getting hacked as well.

And I am just wondering is there a bigger—is there a bigger mission here that we should be pursuing, Ms. Buolamwini, in terms of—you know, I believe in the right to be forgotten. I believe in the right not to be surveilled. I believe there should be sanctuary for us that we don't have to be, you know, surveilled all the time.

Is that something you think about as well?

Ms. BUOLAMWINI. Absolutely, and one thing I can credit the Massachusetts bill for addressing is instead of just saying we are going to look at facial recognition they talk about biometric surveillance, right. So we are also talking about voice recognition. We are talking about gait analysis—anything that is remote sensing.

Do we need to be talking beyond facial analysis technologies? Absolutely as well, so let us look at self-driving cars.

There is a study that came out of Georgia Tech showing that for pedestrian tracking self-driving cars were less accurate for darker-skinned individuals than lighter-skinned individuals.

So when we are talking about this realm of human-centric computer vision, it is not just face recognition that should be concerning.

Mr. LYNCH. Ms. Garvie or Ms. Guliani?

Ms. GULIANI. I mean, the ACLU is one of many organizations that have called on Congress to pass baseline consumer privacy legislation, right, which would put guardrails on how private companies deal with your private data, including biometrics.

And so I do think that that is very much needed and I think that that legislation has to include not just protections but real enforcement.

So when your data is misused you have actually an opportunity to go to court and get some accountability.

Mr. LYNCH. Thank you.

Thank you, Mr. Chairman. I yield back.

Chairman CUMMINGS. Mr. DeSaulnier?

Mr. DESAULNIER. Yes, Mr. Chairman, I want to thank you as well and I want to thank the panel. This has been terrific. I want to take some credit. I don't know if it is true or not, but I think we are part of the same book club. I think I suggested the book to Mr. Lynch and it is a fabulous book, "The Age of Surveillance Capitalism."

And since, like Mr. Gomez, I was one of the three people who they say—you showed that I was misidentified, I was hoping I would be misidentified as George Clooney. But, you know, just my perception of myself.

So I want to talk about this as a representative of——

Mr. CONNOLLY. Yes. Uh-huh.

Mr. DESAULNIER. Uh-huh.

[Laughter.]

Mr. DESAULNIER. That was Connolly, right? Denial is not a river in Egypt.

As a representative from the Bay Area and I have watched these tech companies transform, and I conclude Amazon is part of this culture, and I have listened to them talk about disruption as—you know, if I had questions as elected officials—local or state or Federal—when I was inhibiting innovation, and from my perspective in having met with CEOs who one of them once told me when he was asking for my help on something that he didn't want to deal with people like me.

And I laugh because what he was expressing was that people from the government were slow, didn't understand how this culture was transforming the world, and I really think they believe that and bought into it. It is not about the billions of dollars they make.

And my argument including with Amazon yesterday it would be nice if you tried to work with us to do—deal with the societal impacts because you are going to have to deal with them one way or the other.

But the problem now is when I think of—when I was listening to my colleague talk about the Supreme Court cases I think of Louis Brandeis writing his paper on privacy and convincing other justices like Oliver Wendell Holmes that they were wrong about it—was that he said Americans had the right to be left alone.

How can we say that any longer? None of us are left alone. We just—we have news reports—it is a story on Forbes from this month about Echo and Alexa listening to children.

So I really think, Mr. Chairman, and I am so encouraged by what I have heard in a bipartisan way today that we need to stop—that it has gone down too far. We are not starting at a metric where we are just beginning the deployment of this. It has already been deployed.

And to Mr. Lynch's comments, it is being deployed not just for facial recognition but for everything we do. And there are benefits for that and we can see that, but we need a time out societally, as Europe has led us on, to say no.

And the example in San Francisco is interesting, knowing people in local government in San Francisco. When scooters were trying to get permits, it was great what San Francisco did as, you know, the hub of innovation disruption, sort of.

The two companies who actually came and asked permission were the ones who got permission. The ones who didn't were horrified when they were told no, we are not going give you permits to use these.

If you had just come in in the first place—and I think we have a responsibility in government to be more responsive. But they are not even coming halfway.

So, to me, this is a moment for us in a bipartisan way to say stop. There are benefits to the species in this planet. But you need societal input to this, and we have already lost our right to be left alone. They have de facto taken that away from us.

So, Ms. Guliani, could you respond to that a little bit? Because the cultural attitude they are taking, and they will apply it politically vis-&-vis campaigns and other things, because I think they really do believe that they have done no harm and you and I are in the way by raising questions about how they deploy this technology.

Ms. GULIANI. Yes. I mean, I think one of the things that we have seen with some of the private companies is that they are actively marketing some of these uses.

So in the case of Amazon, they were pushing some of the most concerning uses—face recognition, body-worn cameras, right—opening up the possibility of a near-surveillance state.

And so I think that there—they are not passive actors in the system and they should be forced to take responsibility, and that responsibility should include questions about how accurate is their technology, are they disclosing the problems and the real risks, and are they saying no when they should say no.

And I think when it comes to certainly some of the law enforcement uses that really are life and death scenarios, these companies shouldn't be selling to the government in those scenarios, given the risks that we have talked about.

Mr. DESAULNIER. And given the lack of regulatory enforcement, how do we provide civil enforcement for state laws and Federal laws that aren't being enforced, in my view, right now?

Ms. GULIANI. I mean, with regards to the—some of the private companies and the extent to which they have sold this technology, I think there is questions about whether they have been honest in their disclosures and there is certainly, you know, investigation and analysis in that.

I think, more broadly, from a regulatory standpoint, it is really up to Congress and others to say no, we are going to hit the pause button. Let us not roll out this technology before we really understand the harm and before we think about whether there are, frankly, better alternatives that are more protective for privacy and ones that may also have law enforcement benefits.

Mr. DESAULNIER. Thank you. Thank you, Mr. Chairman.

Chairman CUMMINGS. I recognize Ms. Miller for a unanimous consent request.

Ms. MILLER. Thank you, Chairman Cummings.

I ask unanimous consent to enter this letter from Information Technology and Innovation Foundation into the record.

Chairman CUMMINGS. Without objection, so ordered.

Chairman CUMMINGS. Mr. Connolly?

Mr. CONNOLLY. Thank you, Mr. Chairman.

If I can pick up sort of on where we just were, Ms. Guliani. The ubiquity of this technology strikes me. Maybe we have already kind of mostly lost this battle.

Airports increasingly are using facial recognition technology to process passengers in a more expeditious way, correct?

Ms. GULIANI. TSA and CBP have both introduced face recognition plans. They have not done rulemaking, and some of their plans go far beyond what Congress has authorized.

Mr. CONNOLLY. But CLEAR—isn't CLEAR technology already in airports?

Ms. GULIANI. Yes.

Mr. CONNOLLY. Yes. So, I mean, we already have it and are you aware of any restrictions on that private company in terms of how it uses whatever data is collected currently?

Ms. GULIANI. I don't know that company specifically. I think that with regards to the airport use, there are a lot of questions and concerns. For example, requiring Americans to provide their biometric—their face——

Mr. CONNOLLY. Right.

Ms. GULIANI [continuing]. and questions about whether there is a way to opt out. I tried to opt out. It wasn't an easy process——

Mr. CONNOLLY. Yes.

Ms. GULIANI [continuing]. when I was traveling internationally. And there is also questions about, I think, the build out, right. It has been sort of presented as, well, we are just using this to make travel faster. But when you look at some of the documents, some of the use cases are far beyond that——

Mr. CONNOLLY. Okay.

Ms. GULIANI [continuing]. right, to find people of interest, whatever that means.

Mr. CONNOLLY. So I just think that is for further examination as well. What restrictions do exist, if any, on private companies that are using this technology and from a constitutional point of view what restrictions can there be and—or should there be, and I think that is worthy of some examination as well.

Let me ask about a real-life example of the panel. Anyone can answer. But the FBI currently has agreements with various states in terms of driver's license including states that use facial recognition technology for their driver's license.

And I don't know that that is regulated at all. I don't know that the average citizen getting their driver's license or getting it renewed understands that they have tacitly agreed to allow that piece of data to go to a Federal law enforcement agency to be used however they apparently deem fit.

And I wonder if you would comment on that because at one point the FBI was actually urged to determine whether external facial recognition systems are sufficiently accurate to be justified for FBI use and whether they would agree to limit it if it wasn't, and the FBI actually refused to do that—raising questions that we were talking about earlier in terms of misuse or misapplication of the technology.

So what about the FBI and that relationship with states? Should we be concerned?

Mr. ALEXANDER. You know, I don't think that is—it is a good question for the FBI but it is a good question, quite frankly, for both local, state, and Federal law enforcement because in the public safety community we exchange information back and forth with each other on a—on a constant basis.

And in this particular case in which you are referring to, that would not be unusual. The question becomes and the current concern now is that this has been very much unregulated without any oversight whatsoever and in light of the fact that we are looking at a piece of technology that is very questionable and is raising concern as we continue here this afternoon in this hearing.

So I think that that is part of what has to be assessed and further questions that have to be asked from both the Federal, state, and local level in the sharing of this information that is very sensitive and very questionable when it comes around to our constitutional liberties.

That does raise a great deal of concern and that is part of the complexity in this because for me to be effective as a chief of police at a local level a lot of times I am dependent upon my state and Federal partners, and vice versa, because we have seen benefit in that—not so much around facial recognition technology, but just as a whole of being able to share and communicate with each other around those types of things.

Ms. GULIANI. I mean, when it comes to FBI use we should be concerned. I mean, these are systems that have been in place for years, and as your question rightfully pointed out, the FBI is not even acknowledging a responsibility to fully test the accuracy of systems that it is using and relying on.

And that, I think, builds into a larger question of do we really want this massive data base of all of our faces. We are rapidly approaching a place where virtually every adult will have their face in a system that can be searchable by the FBI where face recognition can be used.

Mr. CONNOLLY. Well, and let me just tell you, in the state of Virginia I don't want my face that is on the driver's license in any data base.

[Laughter.]

Chairman CUMMINGS. Mr. Raskin?

Mr. RASKIN. Mr. Chairman, thank you very much.

The witnesses have described a technology of potential totalitarian surveillance and social control, and I want to thank you for calling this extremely important hearing.

And as chair of the Civil Rights and Civil Liberties Subcommittee with my vice chair, Congresswoman Ocasio-Cortez, we will absolutely work with you to followup on this to make sure that we are looking at all the dimensions of our privacy that are threatened by this and similar technologies.

I want to thank all of the wonderful witnesses for their testimony. I want to start with you, Professor Ferguson, because back in the day we wrote a book together and that was in the days when I wrote books. Today, I write tweets. But I am glad that you are still writing books and Law Review articles.

One of the things I know that has interested you a lot is the question of the seat of government and the right of protest and the right to petition for redress of grievances here in the District of Columbia.

And since January 2017 I have been to a lot of protests here. I have been to the Women's March, the Climate March, the Science March, the March for Our Lives, and on and on. And I am won-

dering if people knew that this technology were being deployed by the government and they were being photographed, so and what effect do you think that would have? And let me ask you and then perhaps Ms. Guliani to weigh in on this.

Mr. FERGUSON. It would fundamentally undermine the First Amendment and the right of free expression and our freedom of association. I think it is chilling and a problem and needs to be banned.

Mr. RASKIN. Ms. Guliani, do you agree with that?

Ms. GULIANI. Yes, I couldn't agree more. The last thing we want before someone goes to a protest and exercises their constitutional right is for them to think, am I going to have my face scanned.

Mr. RASKIN. China, seems to me, to be the dystopian path that needs not be taken at this point by our society. It has been leveraging real-time facial recognition technology to implement its social credit score system, which assesses each citizen's economic and social reputation and pins it at a particular number.

Here is the New York Times: "Beijing is embracing technologies like face recognition and artificial intelligence to identify and track 1.4 billion people. It wants to assemble a vast and unprecedented national surveillance system with crucial help from its thriving technology industry."

Ms. Garvie, let me come to you. We are now seeing that most companies that develop facial recognition systems offer also real-time software. Do we know how many of these are selling their technology to government actors in the United States?

Ms. GARVIE. That is right. Most, if not all, companies that market face recognition to law enforcement in the U.S. also advertise the ability to do face surveillance.

We have no idea how widespread this is, thanks to a fundamental absence of transparency. We have limited visibility into what Chicago is doing, what Detroit is doing, Orlando, the Secret Service here in Washington, DC. and in New York, thanks to FOIA records and investigative journalists' work.

But for a vast majority of jurisdictions we have no idea.

Mr. RASKIN. So you cannot estimate how many communities are actually deploying this technology right now?

Ms. GARVIE. No.

Mr. RASKIN. What is the minimum, do you think?

Ms. GARVIE. So we can estimate conservatively that face recognition generally both uses an investigative tool and potentially as a surveillance tool is accessible to, at very least, a quarter of all law enforcement agencies across the U.S.

That is a conservative estimate because it is based on 300 or so records requests where there are 18,000 law enforcement agencies across the country.

Mr. RASKIN. Great.

Ms. Buolamwini, you make some very powerful arguments in your call for a moratorium on the use of this technology. What objections would you anticipate from people who say that there are legitimate law enforcement uses that are actually helping to solve cases and identify suspects and so on?

Ms. BUOLAMWINI. Well, that is the objection, that there is this hypothetical good use case. But we actually have to look at the re-

ality. So the example I gave earlier is in the United Kingdom where they have reported performance metrics you are getting false positive match rates over 90 percent.

So the promise for what it could do for security versus the reality doesn't match up.

Mr. RASKIN. And that is dangerous. That is positively dangerous.

Ms. BUOLAMWINI. Absolutely.

Mr. RASKIN. I mean, one, because you are violating somebody's civil liberties in the most fundamental way, and two, you are leaving the real criminal suspect or the real criminal out there at large because you have chosen the wrong person.

Ms. BUOLAMWINI. True. But I also wanted to touch on your point with 1.4 billion people being surveyed in China. More than China, Facebook has 2.6 billion people, and as Representative Lynch spoke to, it is not just the state surveillance we have to think about.

We have to think about corporate surveillance. So Facebook has a patent where they say because we have all of these face prints, collected often without consent, we can now give you an option as a retailer to identify somebody who walks into the store and in their patent they say, we can also give that face a trustworthiness score.

And based on that trustworthiness score we might determine if you have access or not to a valuable good. So this——

Mr. RASKIN. Facebook is selling this now?

Ms. BUOLAMWINI. This is a patent that they filed as in something that they could potentially do with the capabilities they have. So as we are talking about state surveillance, we absolutely have to be thinking about corporate surveillance as well and surveillance capital——

Mr. RASKIN. And they would say that all of that is built into whatever contract or licensing agreement people spend 10 seconds signing off on when they set up a Facebook account. Is that right?

Ms. BUOLAMWINI. You would not have to consent.

Mr. RASKIN. Yes. Yes.

Mr. Chairman, finally, something interesting of affinity to today's deliberations just took place, which is a number of us—I think you were with me and other members of the Maryland delegation—we signed a letter expressing concern about the China government—Chinese government-owned and controlled businesses getting contracts to run subway systems in America, including in the Nation's capital here, and there have been a lot of both civil liberties and national security concerns raised by it.

And I want to introduce a front-page article from today's Washington Post, "Despite National Security Concerns, GOP Leader McCarthy Blocked Bipartisan Bid to Limit China's Role in U.S. Transit System."

Chairman CUMMINGS. Without objection, so ordered.

Mr. RASKIN. And I yield back. Thank you.

Chairman CUMMINGS. I have not asked my questions. I am going to ask them now. I know it is getting late but I will be brief.

First of all, I want to thank all of you for an excellent presentation. I think you all really laid out the problem. I always tell my staff, tell me what, so what, and now what.

And Professor Ferguson, I want to thank you. The ACLU released documents revealing that the Baltimore County Police Department, which, of course, is part of my district, partnered with the private company Geofeedia to identify individuals protesting the shooting of Freddie Gray in May 2015.

The company stated, and I quote, "Police officers were even able to run social media photos through facial recognition technology to discover rioters with outstanding warrants and arrest them directly from the crowd," end of quote.

To be clear, police officers may have used facial recognition technology on citizens' personal photos from social media to identify and arrest them while they were exercising their First Amendment right to assemble.

As someone who was in the crowd, I find this discovery to be very disturbing.

Professor Ferguson, the Constitution endows us with, quote, "the right of people to peaceably assemble."

So to all of you, how would widespread police use of facial recognition technology at protests affect citizens' right to peaceably assemble?

Mr. FERGUSON. It is fundamentally American to protest and it is fundamentally un-American to chill that kind of protest. What you talk about in Baltimore is a great example of both the problems of public surveillance and then using third party image aggregators like Facebook and other social media groups to do that kind of private surveillance.

Both will chill future protests. It will chill the desire of American citizens to say that their government may have acted inappropriately, and it is a real problem which deserves congressional regulation.

Chairman CUMMINGS. Anybody else?

Mr. ALEXANDER. Yes, sir, and this is what I have been saying from the onset. If this type of technology is not utilized in a ethical moral constitutional type of way, it continues to do exactly what it did to you out there, Congressman, and other people.

It separates the community from its public safety. There is a lack of trust. There is a lack of legitimacy. There is this whole fear of you being a watchdog over me in a warrior sense as opposed to be a guardian of their community.

No one should have been subjected to what you just articulated. That is the wrong use of this technology, particularly when you have individuals, that was just very eloquently stated by Mr. Ferguson, who are trying to just do normal work and exercise their First Amendment right and for people to be able to assemble and not be subjected to this type of technology, which was used wrongly by Baltimore, and I will say that publicly and privately, because they lacked the training and they lacked the understanding of the potential of what this technology can do to harm their relationship with the community.

That is a serious problem and that is why you have to—for me, here again, these companies that develop this technology they too have to be held responsible and those police departments that acquired that technology from these companies have to be held accountable as well, too.

But after listening myself to much of the testimony that has been stated here today, I really came in here in hopes of being able to say for public safety, for law enforcement itself, there is good use of this technology.

But I think a lot of things that we have talked about now have to be further discovered before we can continue with this technology because my concern, as a former law enforcement official, I don't want technology being utilized by police that is going to separate it further from the community in which it already serves. If there is benefit to it, let us find it. Let us utilize it to help keep our communities safe——

Chairman CUMMINGS. Thank you.

Mr. ALEXANDER [continuing]. and because there is no exception and there is no shortcut around that.

Chairman CUMMINGS. Ms. Guliani, let me ask you the same. We have had a lengthy discussion here. But I have heard very little about court cases and I was kind of surprised that I haven't.

Has this been tested? I mean, have we—are there court where—has this been an issue and are there court cases with regard to this?

Because it does seem to me that the ranking member made some good points that you have got people at the FBI making agreements with police departments, nobody elected in the process, and they are using this stuff, and then you have all the arguments that you all have made with regard to the defectiveness of the—of the machinery.

What has happened on that front?

Ms. GULIANI. Sure. There is no court of appeals that has directly addressed the constitutionality of, let us say, real-time face recognition or matching against a driver's license data base.

And I think that one of the big reasons for that is for defendants to raise that challenge they have to be notified, and people aren't being notified.

And so I think that that is insulating this technology from the judicial review that is very sorely needed. Having said that, there is, obviously, other bodies of case law—the Carpenter decision and others—which are relevant and could apply to uses of face recognition.

But what we need is notice so that these cases can come before the court. Without that, it becomes very difficult to have developed case law.

Ms. BUOLAMWINI. One way people are getting notice is by having economic opportunity denied. So May 20 this week you actually have William Fambrough, who is in Missouri, who submitted a case against Uber Technologies, and the reason for doing this is because Uber requires a selfie verification to make sure you are the driver you say you are, and in his particular case, because he was having to lighten his photos so he could be recognized, Uber said he doctored the photos and unilaterally kicked him off the platform with no kind of recourse.

So this was just filed. I don't know how it will go through. But, again, the only reason the person knew was because they no longer had this access to economic opportunity.

Chairman CUMMINGS. Coming back to you, Dr. Alexander, how do you think the use of facial recognition technology to survey crowds is changing police tactics?

And one of the things I noticed in Baltimore is that they—you know, at one time—I think they still do it—have a—use a helicopter and they take these images.

And how does that relate to all of this. You know what I am talking about?

Mr. ALEXANDER. Yes, and you are also talking about drone technology, I would imagine.

Chairman CUMMINGS. Yes. Yes.

Mr. ALEXANDER. Yes, sir. Well, you know, a lot of this is still—in many ways, it is very early stages. But I still think it goes back to the entire privacy issues.

But one of the biggest things I find, Chairman, from my experience is that when new technology is developed and we take that technology and we introduce it into our communities across the country, we never tell our communities what it is, why it is being utilized, and how it would help benefit public safety.

So what ends up happening is people draw their own conclusions around it, already sometimes in suspicion of the work that police are doing because oftentimes they operate in a very clandestine type of sense.

But I think it is important as this technology continues to emerge, whether we are using air support with infrared cameras or whether we are using drone technology or whatever the case may be, as we continue to evolve in our technology, when that technology comes to my front door, as a law enforcement official I want to know all about it. I want to ask all the right questions.

I want to have the type of people that are at the table right here with us today to ask the appropriate questions so we are going to advance this technology and be able to educate my community in terms of what it means and what is the benefit of it and what is the challenges that are associated with it.

It makes that type of technology much better for people to digest and be able to understand and, as we run across problems that evolve as a result of it, we are able to work with our communities to help resolve those even if we have to enact new legislation around it.

Chairman CUMMINGS. But an hour ago you said that you were not anxious to see a moratorium and it sounds like you may have changed that a little bit.

Mr. ALEXANDER. Well, I mean—I mean, I am not because, you know, one thing I support, Chairman, I support technology. But I support good technology and I support technology that has rules with it and it has oversight with it and there is policies written around it.

I, certainly, would rather not see a moratorium. However, if the issues that have been articulated here today are as serious as we believe they to be, then we have to go back and ask ourselves that question.

But here is the thing we have to be cautious of. If we are going to put a moratorium on this technology, I also want to hear what have been the benefits, if any—if any. What have been the benefits

and how do we utilize some of those benefits in some type of constructive way until we work out the bigger problems around the issues that we have discussed here today.

I just don't want to throw the baby out with the bathwater if there is some way in which this technology, which I am going to make a reasonable assumption and based on my own experience in some ways it has been useful.

But if it is going to continue to harm the American people, then it is certainly something in which we need to consider putting some pause to, if you will, in being able continue to investigate what is the good part of this technology if possible we still can utilize as we go through this process of learning more and putting legislation around it.

Chairman CUMMINGS. Ms. Guliani, you had something to say?

Ms. GULIANI. Yes. I mean, I think that we have to resolve some of the fundamental questions and problems. How are going to prevent this technology from having a disparate impact either because of accuracy or because of existing biases in the criminal justice system?

How are we going to prevent the buildup of a surveillance state, right, where there is a camera on every street corner and people don't feel like they can walk around anonymously?

How are we going to safeguard our First Amendment liberties and make sure that no one says to themselves, I can't go to this protest because I am afraid my face is going to be scanned?

And so I think before—we can't move forward with this technology until we can answer and resolve those fundamental questions.

Chairman CUMMINGS. Ms. Cortez, did you have anything? Anybody else?

Ms. OCASIO-CORTEZ. Yes. I mean, first of all, Mr. Chairman, I want to thank you again for holding this hearing. It is so critical that part of our operation here as government and part of, as Mr. DeSaulnier expressed, is making government responsive and making sure that we are ahead of the curve so we are not consistently operating out of a reactive space but out of a proactive space.

Because there are forces out there. Whether it is a corporation trying to make and squeeze a dollar out of every bit of information about your life or whether it is foreign governments trying to hack these data bases for that information as well, we need—there are folks out there that know the kind of world they want to create that advances their interests and I think that it is extraordinarily encouraging that this is a strong bipartisan issue.

Whether we are concerned about this for—whether we are concerned about this for a civil liberty reason, whether we are concerned about this for criminal justice reform reasons, about right to privacy, this is about who we are as America and the America that is going to be established as technology plays an increasingly large role in our societal infrastructure.

And we have to make sure how American values and our Bill of Rights and our constitutional protections get translated to the internet and in the digital age.

So I want to thank all of our witnesses for coming here. I want to thank the chairman for your foresight in holding this hearing. We got to get something done.

Chairman CUMMINGS. And we will.

Ms. OCASIO-CORTEZ. And I look forward to working with the—you know, our colleagues on the other side of the aisle and many of the caucuses that have aligned around these basic principles.

Chairman CUMMINGS. Mr. Gomez?

Mr. GOMEZ. Mr. Chairman, I want everybody to be very clear. We are not anti-technology and we are not anti-innovation.

But we got to be very aware that we are not stumbling into the future blind and at that same time giving up some liberties and protections that we have all cherished not only for decades but for generations.

It is always that balance between innovation and protecting individual rights and civil liberties. We get that. But this is a issue that I think must be looked at. As I said, I was never planning on working on this issue. the issue found me. Well, thank you to the ACLU.

At the same time, I just got word that the shareholders did not end up passing a ban—of Amazon did not pass a ban on the sale of recognition. And you know what? That just means that it is more important that Congress acts.

So with that, I yield back, and thank you, Mr. Chairman, for your leadership.

Chairman CUMMINGS. Thank you.

Without objection, the following statements will be included in the hearing record: Project on Government Oversight report titled "Facial Recognition: Facing the Future of Surveillance; No. 2, Electronic Privacy Information Center letter on the FBI's next-generation identification program; No. 3, Geofeedia case study titled, quote, "Baltimore County Police Department, Geofeedia Partner to Protect the Public During Freddie Gray Riots," end of quote.

Chairman CUMMINGS. Did you have something, Mr. DeSaulnier?

Mr. DESAULNIER. No. Thank you.

Chairman CUMMINGS. Very well.

I would like to thank our witnesses. This has been—I have been here for now it is 23 years. It is one of the best hearings I have seen, really. You all were very thorough and very detailed.

Without objection, all members will have five legislative days within which to submit additional written questions for the witnesses to the chair, which will then be forwarded to the witnesses for their—a response.

I ask all witnesses to please respond as promptly as you can. Again, I want to thank all of you for your patience. Sorry we got started late. We had some meetings, and we have gone on for a while.

But thank you very much.

This meeting is adjourned.

[Whereupon, at 1:23 p.m., the committee was adjourned.]

○