AUTHENTICATED
U.S. GOVERNMENT
INFORMATION
GPO

S. HRG. 116–629

THE INVALIDATION OF THE EU-U.S. PRIVACY SHIELD AND THE FUTURE OF TRANSATLANTIC DATA FLOWS

HEARING

BEFORE THE

COMMITTEE ON COMMERCE, SCIENCE, AND TRANSPORTATION UNITED STATES SENATE

ONE HUNDRED SIXTEENTH CONGRESS

SECOND SESSION

DECEMBER 9, 2020

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

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

U.S. GOVERNMENT PUBLISHING OFFICE
52–856 PDF WASHINGTON : 2023

SENATE COMMITTEE ON COMMERCE, SCIENCE, AND TRANSPORTATION

ONE HUNDRED SIXTEENTH CONGRESS

SECOND SESSION

ROGER WICKER, Mississippi, *Chairman*

JOHN THUNE, South Dakota
ROY BLUNT, Missouri
TED CRUZ, Texas
DEB FISCHER, Nebraska
JERRY MORAN, Kansas
DAN SULLIVAN, Alaska
CORY GARDNER, Colorado
MARSHA BLACKBURN, Tennessee
SHELLEY MOORE CAPITO, West Virginia
MIKE LEE, Utah
RON JOHNSON, Wisconsin
TODD YOUNG, Indiana
RICK SCOTT, Florida

MARIA CANTWELL, Washington, *Ranking*
AMY KLOBUCHAR, Minnesota
RICHARD BLUMENTHAL, Connecticut
BRIAN SCHATZ, Hawaii
EDWARD MARKEY, Massachusetts
TOM UDALL, New Mexico
GARY PETERS, Michigan
TAMMY BALDWIN, Wisconsin
TAMMY DUCKWORTH, Illinois
JON TESTER, Montana
KYRSTEN SINEMA, Arizona
JACKY ROSEN, Nevada

JOHN KEAST, *Staff Director*
CRYSTAL TULLY, *Deputy Staff Director*
STEVEN WALL, *General Counsel*
KIM LIPSKY, *Democratic Staff Director*
CHRIS DAY, *Democratic Deputy Staff Director*
RENAE BLACK, *Senior Counsel*

CONTENTS

WITNESSES

APPENDIX

THE INVALIDATION OF THE EU-U.S. PRIVACY SHIELD AND THE FUTURE OF TRANSATLANTIC DATA FLOWS

WEDNESDAY, DECEMBER 9, 2020

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

The Committee met, pursuant to notice, at 10:02 a.m., in room SR–253, Russell Senate Office Building, Hon. Roger Wicker, Chairman of the Committee, presiding.

Present: Senators Wicker [presiding], Thune [presiding], Blackburn, Scott, Cantwell, Blumenthal, Schatz, Peters, and Rosen.

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

The CHAIRMAN. Good morning, and welcome to today's hearing on the "Invalidation of the EU-U.S. Privacy Shield and the Future of Transatlantic Data Flows". I extend a special welcome to our distinguished panel of witnesses and thank them for appearing today.

Today we will hear from Mr. James Sullivan, Deputy Assistant Secretary for Services with the International Trade Administration at the Department of Commerce; the Honorable Noah Phillips, Commissioner at the Federal Trade Commission; Ms. Victoria Espinel, President and Chief Executive Officer at BSA; the Software Alliance, Mr. Peter Swire, who is the Elizabeth and Tommy Holder Chair of Law and Ethics at the Georgia Tech Scheller College of Business and Research Director at the Cross-Border Data Forum; and Mr. Neil Richards, Koch Distinguished Professor of Law at Washington University and St. Louis School of Law.

And I assume Mr. Richards is appearing by video. I have been told that. That is great. Data is the lifeblood of the global digital economy. Free movement of data across national borders underpins trillions of dollars of international trade, commerce, and investment. Data serves as a catalyst for innovation, productivity, and economic growth, and helps promote U.S. competitiveness in technology leadership around the world. According to one estimate, digitally-enabled trade amounted to between $800 and $1,500 billion globally in 2019, and is projected to raise global GDP by over $3 trillion this year. To sustain digital trade and the free flow of data, governments have sought to eliminate trade barriers and safeguard the privacy and security of consumers' personal data, a top priority of this committee.

Maintaining a shared commitment to protecting consumers' personal data has been particularly important to our trade relationship with Europe. In 2016, the United States and the European Union agreed to the Privacy Shield framework. This framework established a legal mechanism to provide for transfer of EU citizens' personal data to the United States in compliance with EU data protection laws. The establishment of the Privacy Shield was intended to ensure that over 5,000 small and medium sized businesses spanning several economic sectors in both the U.S. and EU could continue engaging in transatlantic digital commerce without disruption.

Among other things, the Privacy Shield required participating organizations to give notice about their collection and use of the data of EU citizens, and give individuals the right to opt out of having their personal information disclosed to a third party. Organizations were also required to implement effective redress mechanisms for EU citizens to file complaints about how their data is used outside of the EU. And the United States was required to appoint an ombudsperson at the State Department to ensure complaints were properly investigated. The Privacy Shield included additional assurances that there would be clear conditions, limitations, and active oversight concerning Government access to EU citizens' personal data for National Security purposes. In July of this year, the European Court of Justice invalidated the Privacy Shield, and that is the reason we are here today, citing inadequate data protections in the U.S. based on our surveillance laws and an alleged lack of redress rights for EU citizens in the United States.

Today's hearing is an opportunity to discuss what can be done to develop a durable and lasting data transfer framework between the United States and the EU that provides meaningful data protections to consumers, sustains free flow of information across the Atlantic, and encourages continued economic and strategic partnership with our European allies. A tall order, but an essential order. A solution begins with understanding the underlying issues that led to the invalidation of the Privacy Shield this summer. I hope our witnesses will discuss the merits of the Privacy Shield to redress rights for EU citizens and how U.S. intelligence practices compare to those of the EU member states.

I also look forward to witnesses addressing how the invalidation of the Privacy Shield affects the viability of other data transfer mechanisms. To take one example, in a mechanism called Standard Contractual Clauses, exporters of EU citizens? data to the U.S. now have to carry out an assessment of whether U.S. law provides adequate protections. The EU's Data Protection Board recently issued guidance on how to comply with EU law while relying on standard contractual clauses to transfer data across the Atlantic. But in issuing this guidance, the EU Data Protection Board acknowledged that the implementation of these measures may still be insufficient to transfer data legally to the U.S. and other non-EU countries.

With this in mind, I hope witnesses will discuss how U.S. businesses can confidently conduct transatlantic data transfers in compliance with EU laws as we continue bilateral negotiations to replace the Privacy Shield. I welcome the European Commission's commitment to continue working with the United States to ensure

continuity of safe data flows in a manner that reflects the values we share as democratic societies. And I had a very productive and informative conversation with members of the European Commission just yesterday.

Finally, a major priority of this committee has been strengthening consumer data privacy through the development of bipartisan Federal data privacy law. I look forward to witnesses discussing how a comprehensive data privacy law with strong enforcement and meaningful privacy and redress rights for consumers might be able to aid efforts to develop a successor data transfer framework between the United States and the EU.

Having said that mouthful and gone 3 minutes over, I thank you for your participation and I turn to my dear friend and colleague, Ranking Member Cantwell, for her opening remarks.

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

Senator CANTWELL. Thank you, Mr. Chairman, and thank you for holding this hearing. Also, thank you for your leadership on the Helsinki Commission. I certainly appreciate your hard work in both of those roles and trying to solve and—resolve these issues between the United States and the European Union. So I also want to thank our colleagues, Senators Cardin and Shaheen, for also working on that Helsinki Commission and these important issues. The decision by the European Court of Justice earlier this summer makes it abundantly clear we need to have a new agreement between the United States and Europe to address the transatlantic data flow. It must be a top priority by the Biden Administration. We must ensure the continued free flow of commercial data between the United States and Europe.

When I think about the Mexico Free Trade Agreement and getting the digital provisions in there, this is something that is now the norm. This is not an obscure thing. It is going to become more and more and more about trade and figuring out trade. Trade is digital. So a lot is at stake. The U.S. and EU digital trade is worth more than $300 billion annually, including more than $218 billion in U.S. exports to Europe. So a very important export issue. And every business that exports and imports, has a presence or investment in the U.S. and Europe will face difficulties if there are barriers to cross-border data transfer. In all, more than $1 trillion in U.S.-European trade is at risk.

With the invalidation of the Privacy Shield Agreement, we now have lost the most straightforward legal tool for transferring data from the EU to the US. And this is a particular problem for small and medium sized businesses. It also puts some of our largest and more sophisticated companies at a disadvantage and cast doubt on the protection of their digital services and what they provide. Europe and the United States have had a long history of working together, and to address our global challenges and security issues at the same time, we must redouble those efforts.

We must continue to work closely to defend our shared values for democracy and the rule of law. And I want to see the U.S. and Europe working together on these very important national concerns, trade and technology, so that we can continue to improve economic

opportunities and avoid moves toward protectionism. We need to start by coming together on protecting data, but we also must increase bilateral cooperation on a broad digital agenda, 5G, 6G, a regulatory framework for artificial intelligence, autonomous vehicles, cybersecurity-disinformation standards. So I support the European proposal to create a US, European Technology Council for dialogue. Maybe the Commission, the Helsinki Commission and others can help on this.

We can work together in a multilateral organizations like OECD and the G7 to confront the challenges from China and Russia so that we can more focus on what the standards are for the next generation of technology and to ensure for the proper protection of intellectual property. This must be our larger goal. If we fail to increase our cooperation on digital issues, our economy will suffer the consequences. The free flow of data between the United States and Europe is especially critical to 5,000-plus tech companies in the State of Washington, which generate more than $2.8 billion in digital export. And so equally important here today are the privacy issues that we are still working on as a committee.

These are important issues. So we don't want consumers left behind. We want them to have control over their personal, privacy data. We want, at the State and Federal level, to make sure that we have the right safeguards in place for consumers. So I guarantee you the United States and European citizenry are on the same page. These are the concerns that we all share, that the U.S. may have, at a Government level, a bulk collection of intelligence information that might violate those privacy rights. So we have to work hard to resolve this issue of the Privacy Shield and work hard on privacy legislation next year.

So thank you, Mr. Chairman. I look forward to working with you in resolving the issues between us on our two bills, and certainly we have made progress. It is a very hard issue. But the digital world is not going away, so we have to not only pioneer it, but pioneer the laws and safeguards that go along with it. Thank you very much.

The CHAIRMAN. And thank you for that very fine statement, Madam Ranking Member. And we now have an opportunity for opening statements by our distinguished panel. Prepared statements will be submitted and included in full in the record at this point, and we ask each witness to summarize in 5 minutes or less.

Let me also say, we have a vote—we have a series of three roll call votes at 11 a.m., and I think what we will do, Senator Cantwell, is just continue the hearing and we will ask members, two members of the Committee to preside while we go back and forth.

Three, 15 minute votes, takes us well over an hour in the U.S. Senate. So we would be advised that that will not be a particularly steep hill for us to climb. Mr. Jim Sullivan, what do you have to tell us in 5 minutes? You bet, yes.

STATEMENT OF JAMES M. SULLIVAN,
DEPUTY ASSISTANT SECRETARY FOR SERVICES,
INTERNATIONAL TRADE ADMINISTRATION,
U.S. DEPARTMENT OF COMMERCE

Mr. SULLIVAN. Good morning, Chairman Wicker, Ranking Member Cantwell, distinguished members of the Committee. Thank you for the invitation to testify about the EU-U.S. Privacy Shield Framework and the recent *Schrems II* decision by the Court of Justice of the European Union. I am heartened by your bipartisanship on the importance of cross-border data flows. I appreciate the Committee's very active engagement on Privacy Shield and the five months since the court's ruling.

As the Deputy Assistant Secretary for Services in the International Trade Administration, I oversee the Office of Digital Services Industries and the team responsible for U.S. Government, administration, and oversight of the Privacy Shield framework. During the 3-year period between July 2017 and July 2020, the Privacy Shield team and I led three successful joint annual reviews of the functioning of the framework with our partners in the European Commission and European data protection authorities. We also facilitated a 125 percent increase in the number of Privacy Shield participants, from 2,400 to 5,400 companies, that relied on the framework to conduct transatlantic trade.

Our Office of Digital Services Industries has long advocated for policies that support the free flow of data across borders as essential to global commerce, and I welcome this opportunity to comment on the status of transatlantic data flows today. And with the growth in Internet connectivity and the accelerating digitization of the global economy, cross-border data flows have become just as important to growing American jobs and competitiveness as U.S. trade in goods and services. Because the United States has been a preeminent innovator and early adopter of information and communications technology, our Nation occupies a singular leadership role in the digital economy today.

With the July 16th decision in the *Schrems II* case, however, data transfers from one of our largest trading partners are now under serious threat. In addition to invalidating the European Commission's adequacy decision for the Privacy Shield framework, *Schrems II* decision has also called into question the reliability of other key mechanisms for moving personal data from Europe to the United States.

That ability to transfer data, including personal data, seamlessly across borders generates enormous benefits for our Nation. It affords Americans greater opportunities and a better quality of life by allowing us all to interact with people in organizations anywhere in the world. It allows our businesses, no matter how large or small, to use the Internet to market and deliver their goods and services wherever data is allowed to flow. And with technologies like 5G, the Internet of Things, and AI, the next wave of digital innovation is already here and the ability to transfer data across borders is an essential driver of innovation, competitiveness, and economic growth.

At this particular moment in history, moreover, international data flows enable the data sharing and collaborative research crit-

ical to understanding the COVID-19 virus, to mitigating its spread, and to expediting the discovery and the development of treatments and vaccines. The United States and the European Union enjoy a $7.1 trillion economic relationship with $5.6 trillion in transatlantic trade annually. By some estimates, nearly $450 billion of this trade involves digital services.

In truth, given the ongoing digitization of virtually every sector of our economy and the fact that transatlantic data flows are the highest in the world, far more of that $5.6 trillion in trade is facilitated in some fashion by cross-border transfers of data. Now, despite our shared recognition of the importance of privacy and data protection, the United States and the European Union do differ in our respective legal approaches. As a general matter, the United States has adopted a sectoral approach to privacy with Federal laws focused on protecting certain types of particularly sensitive data, such as financial or medical information.

The European Union, by contrast, largely protects all personal data under a single set of rules set forth in one law, the General Data Protection Regulation, or GDPR. And it prohibits companies from transferring EU personal data outside Europe, except under special circumstances. Transfers are expressly permitted to a recipient in a third country, for example, if the European Commission has determined that the laws of that country provide an adequate level of data protection, which is essentially equivalent to that afforded under EU law. If there is no adequacy decision for a country, a company may still transfer EU personal data to a recipient in that country by using an EU-approved data transfer mechanism.

As the European Commission has not made an adequacy decision for the United States, the primary transfer mechanisms used by U.S. companies have been standard contractual clauses, or SCCs, and until recently, Privacy Shield. Privacy Shield was negotiated as a successor to the 15 year old Safe Harbor Framework, which itself was invalidated by the EU Court of Justice in the 2015 *Schrems I* case in the wake of the Snowden disclosures. Finalized in July 2016, Privacy Shield created the ombudsperson mechanism at the State Department to investigate certain requests from EU individuals related to U.S. National Security access to their personal data. Because the privacy——

The CHAIRMAN. Mr. Sullivan, we are going to put your whole statement into the record. If you could summarize in 30 more seconds so we can move along.

Mr. SULLIVAN. Sure. As framed by the court, the central question in *Schrems II* was whether in view of U.S. law and practice regarding Government access to personal data for National Security purposes, Privacy Shield and SCCs provide sufficient safeguards to EU personal data transferred to the United States? Although the European Commission and several EU member states joined the U.S. Government in arguing that U.S. law and practice do, in fact, satisfy EU data protection standards, the court answered the question with respect to Privacy Shield with a definitive, no.

And that ruling has created enormous uncertainties for U.S. companies and the transatlantic economy at a particularly precarious time. Effective immediately, the 5,400 Privacy Shield participants

could no longer rely on the framework as a basis for transferring personal data. And because neither the court nor the European data protection authorities provided for any enforcement grace period, these companies were basically left with three choices: they could do nothing and risk huge fines for violating GDPR, they could withdraw from the European market altogether, or they could switch right away to other more expensive data transfer mechanisms——

The CHAIRMAN. OK, we will take the rest of the statement for the record.

Mr. SULLIVAN. Thank you.

[The prepared statement of Mr. Sullivan follows:]

PREPARED STATEMENT OF JAMES M. SULLIVAN, DEPUTY ASSISTANT SECRETARY FOR SERVICES, INTERNATIONAL TRADE ADMINISTRATION, U.S. DEPARTMENT OF COMMERCE

1. INTRODUCTION

Good morning, Chairman Wicker, Ranking Member Cantwell, and distinguished Members of the Committee.

Thank you for the invitation to testify about the EU–U.S. Privacy Shield Framework and the recent *Schrems II* decision by the Court of Justice of the European Union. I am heartened by your bipartisanship on the importance of cross-border data flows and appreciate the Committee's active engagement on Privacy Shield in the five months since the Court's ruling.

As the Deputy Assistant Secretary for Services in the International Trade Administration, I oversee the Office of Digital Services Industries and the team responsible for U.S. Government administration and oversight of the Privacy Shield Framework. During the three-year period between July 2017 and July 2020, the Privacy Shield Team and I led three successful joint annual reviews of the functioning of the Framework with the European Commission and European data protection authorities, and facilitated a 125 percent increase in the number of Privacy Shield participants—from 2,400 to 5,400 U.S. companies that relied on the Framework to conduct transatlantic trade.

The International Trade Administration's Office of Digital Services Industries has long been focused on digital trade and data governance issues, advocating for policies that support the free flow of data across borders as essential to global commerce. As such, I welcome this opportunity to comment on the status of transatlantic data flows today.

With the growth in Internet connectivity and accelerating digitization of the global economy, cross-border flows of data have become just as important to growing American jobs and global competitiveness as U.S. trade in goods and services. Because the United States has been a preeminent innovator and early adopter of information and communications technology, our Nation occupies a singular leadership role in the digital economy today.

With the July 16, 2020 decision by the Court of Justice of the European Union in the *Schrems II* case, however, data transfers from one of the United States' largest trading partners are now under serious threat. In addition to invalidating the European Commission's adequacy decision for the EU–U.S. Privacy Shield Framework, the *Schrems II* decision has also called into question the reliability of the other key mechanisms for moving personal data from Europe to the United States.

My testimony will first explore why transatlantic data flows are so important to the U.S. economy. I will then review briefly the differing regulatory approaches to data privacy in the United States and the European Union, and how we have managed to bridge those differences in the past through innovative frameworks like Privacy Shield. Finally, I will discuss the *Schrems II* decision, its implications for U.S. businesses, and the Administration's efforts to restore legal certainty around transatlantic data flows by negotiating mutually acceptable standards of data privacy through targeted enhancements to the Privacy Shield Framework.

At the outset, I should note that I am limited as to what details I can share at this time with respect to discussions with the European Commission.

2. IMPORTANCE OF TRANSATLANTIC DATA FLOWS

The ability to transfer data—including consumers' personal data—seamlessly across borders generates enormous benefits for our citizens, our businesses, and our Nation.

It affords Americans greater opportunities and a better quality of life—by allowing us all to interact with people and organizations anywhere in the world and access an ever-growing number of goods and services that can be tailored to our individual needs and preferences.

It allows our businesses, no matter how large or small, to use the Internet to more easily market and deliver their ideas, goods and services—wherever data is allowed to flow. Today, solo entrepreneurs and small- and medium-sized enterprises can reach global markets—and the 4.5 billion people now connected to the Internet—with unprecedented ease. American businesses of all sizes in every industry rely on personal data to facilitate transactions; enhance efficiencies; reduce costs; generate new customer insights; improve the quality of products and services; prevent and mitigate fraud; and manage their international networks of employees, customers, and suppliers.

With technologies like 5G, the Internet of Things, robotics, and artificial intelligence, the next wave of digital innovation is already here, and the ability to transfer data across borders—to and from Europe and other places in the world—is an essential driver of commercial competitiveness, economic growth, innovation, job creation, and wage growth worldwide. The economic benefits are clear not only for the United States but for Europe itself. At this particular moment in history, moreover, international data flows enable the data sharing and collaborative research critical to understanding the COVID–19 virus, mitigating its spread, and expediting the discovery and development of treatments and vaccines.

The United States and the European Union enjoy a $7.1 trillion economic relationship—with $5.6 trillion in transatlantic trade annually. According to some estimates, nearly $450 billion of this trade involves digital services. In truth—given the ongoing digitization of virtually every industry sector and the fact that cross-border data flows between the U.S. and Europe are the highest in the world—far more of that overall $5.6 trillion in trade is facilitated in some way by cross-border transfers of data.

3. DIFFERENT APPROACHES TO DATA PRIVACY

Despite our shared recognition of the importance of consumer privacy and data protection, the United States and the European Union differ in our respective legal approaches.

As a general matter, the United States does not have one comprehensive data protection or privacy law. Privacy is regulated through a number of laws enacted at the Federal and state level. Federal laws often vary considerably in their purpose and scope. Many Federal laws impose data protection requirements tailored to specific sectors, such as finance, health, and communication. Several Federal laws focus on protecting certain types of particularly sensitive and at-risk consumer data. These include an individual's financial and medical information; children's online information; background investigations and "consumer reports" for credit or employment purposes; and certain other specific categories of data. All 50 states have also enacted legislation requiring private or governmental entities to notify individuals of security breaches of personally identifiable information.

The European Union, by contrast, largely protects *all* personal data under a single set of rules set forth in one law—the General Data Protection Regulation or "GDPR."

As a general matter, EU law also prohibits a company from transferring EU personal data outside Europe except under special circumstances.

First, transfers are expressly permitted to a recipient in a third country if the European Commission has determined that the national laws of that country provide an "adequate level of protection" for personal data which is "essentially equivalent" to the level afforded under EU law. There are only 12 jurisdictions in the entire world that the European Commission currently considers to ensure an adequate level of protection: Andorra, Argentina, Canada, Faroe Islands, Guernsey, Israel, Isle of Man, Jersey, New Zealand, Switzerland, Uruguay, and Japan.

And second, if there is no adequacy decision for a country, a company may still transfer EU personal data to a recipient in that country by using an EU-approved "transfer mechanism" that ensures sufficient data protection by the recipient. Standard Contractual Clauses or "SCCs" are the main transfer mechanism used by 90 percent of companies that transfer EU personal data internationally. Another option, Binding Corporate Rules or BCRs, is a set of legally enforceable internal policies for data transfers *within* a group of enterprises, typically large multinational organizations. Owing to a lengthy and expensive approval process, however, relatively few organizations—only about a hundred around the world—have adopted BCRs.

As the European Commission has not made an adequacy decision for the United States as a whole, the primary EU-approved data transfer mechanisms used by U.S. companies have been SCCs and, until recently, the EU–U.S. Privacy Shield, which was a "partial" adequacy decision in that it only covered transfers to Privacy Shield-certified companies in the United States.

The EU-U.S. Privacy Shield Framework

Privacy Shield was negotiated as a successor to the 15-year old Safe Harbor Framework. Under Safe Harbor, over 4,000 U.S. companies made legally enforceable promises that allowed for the transfer of EU personal data to the United States in compliance with EU law. In 2013, Austrian data privacy activist Max Schrems challenged Safe Harbor, and in 2015—spurred by Edward Snowden's unauthorized disclosures of national security information—the Court of Justice of the European Union invalidated the European Commission's adequacy decision that had underpinned the Framework since 2000.

To address the *Schrems I* decision, and in anticipation of GDPR's implementation in 2018, the Department of Commerce and its interagency partners worked with the European Commission to develop and maintain a modernized and durable transatlantic data protection framework. After months of intense negotiations, the United States and the European Commission finalized the EU–U.S. Privacy Shield Framework in July 2016.

Under the terms of the new Framework, the United States created the Privacy Shield Ombudsperson Mechanism at the State Department to investigate certain requests from EU individuals related to national security access to EU personal data transmitted to the United States. Because the Privacy Shield Ombudsperson Mechanism applied to EU personal data transmitted to the United States pursuant to *any* transfer tool approved under EU law (including SCCs and BCRs), Privacy Shield became a key enabler of *all* transfers of EU personal data to the United States.

The International Trade Administration's Privacy Shield Team serves as the interagency lead for the Framework and administers the day-to-day functioning of the Privacy Shield Program. It works with eligible organizations seeking to certify to the Framework by verifying that they have developed a Privacy Shield-compliant privacy policy; identified an independent recourse mechanism to investigate complaints; contributed to an arbitration fund; implemented compliance procedures; and designated a representative to handle questions, complaints, data access requests, and other issues related to the organization's participation in the Program.

Once the Privacy Shield Team finalizes an organization's certification, it then adds that organization to the public-facing "Privacy Shield List". This list enables European companies or other interested parties to verify whether data can be transferred to the organization under the Framework.

An organization's public commitments to abide by the Framework's requirements are legally enforceable. Accordingly, to support the integrity of the Program, the Privacy Shield Team monitors organizations' compliance and potential "red flags" on an ongoing basis—and refers matters that may warrant further investigation to the Federal Trade Commission or the Department of Transportation for potential enforcement action as necessary.

In addition, each year since 2017, senior U.S. and EU officials have convened to conduct intensive two-day reviews of the functioning of the Privacy Shield Program. As noted earlier, the Privacy Shield Team and I led three successful annual reviews of the Program together with the European Commission, European data protection authorities, and U.S. Government colleagues from the Departments of State, Justice, and Transportation, the Office of the Director of National Intelligence, the Federal Trade Commission, and the Privacy and Civil Liberties Oversight Board, among others.

Our regular interactions with EU officials before, during, and after these annual Privacy Shield reviews afforded numerous constructive opportunities for transatlantic coordination and cooperation on promoting trust in the digital economy. Following the third annual review in Washington, DC in October 2019, for example, European Commissioner for Justice Věra Jourová enthusiastically acclaimed Privacy Shield a "success story".

For four years, Privacy Shield was the most straightforward and cost-effective EU-approved transfer mechanism for U.S. and European companies of all sizes in virtually every industry. For many firms—and for small- and medium-sized firms especially—Privacy Shield was often the *only* viable data transfer mechanism. Many such firms simply do not have the resources or administrative capacity to utilize more costly and burdensome mechanisms like SCCs or BCRs. Of the 5,400 Privacy Shield participants on July 16, 2020, over 70 percent were small-and medium-enterprises with fewer than 500 employees.

4. *SCHREMS II*

The July 16, 2020 *Schrems II* decision was the latest development in a long-running legal battle that has been waged in the Irish courts and the EU Court of Justice by Max Schrems. As framed by the Court, the central question in the case was whether—in view of U.S. law and practice regarding government access to personal data for national security purposes—Privacy Shield and SCCs provided sufficient safeguards to EU personal data transferred to the United States. Although the European Commission and several EU Member States joined the U.S. Government in arguing that U.S. law and practice *do* in fact satisfy EU data protection standards, the Court answered the question with respect to Privacy Shield with a definitive "no".

The Court based its decision on two principal grounds. First, after analyzing the European Commission's 2016 adequacy decision for Privacy Shield, it found that certain U.S. intelligence access to EU personal data transferred under the Framework was not constrained in a way that satisfies the EU's legal requirement for "proportionality". Second, the Court concluded that the Privacy Shield Ombudsperson Mechanism did not afford sufficient redress for violations of EU individuals' right to data protection.

The *Schrems II* decision has created enormous uncertainties for U.S. companies and the transatlantic economy at a particularly precarious time. Immediately upon issuance of the ruling, the 5,400 Privacy Shield participants and their business partners in the EU could no longer rely on the Framework as a lawful basis for transferring personal data from Europe to the United States. Because neither the Court nor European data protection authorities provided for any enforcement grace period, Privacy Shield companies were left with three choices: (1) risk facing potentially huge fines (of up to 4 percent of total global turnover in the preceding year) for violating GDPR, (2) withdraw from the European market, or (3) switch right away to another more expensive data transfer mechanism.

Unfortunately, because of the Court's ruling in the Privacy Shield context that U.S. laws relating to government access to data do *not* confer adequate protections for EU personal data, the use of other mechanisms like SCCs and BCRs to transfer EU personal data to the United States is now in question as well.

Since the *Schrems II* decision, the lack of legal clarity regarding data transfers from Europe to the United States has prompted some companies to begin considering data localization in Europe. Storing and processing *all* EU personal data in Europe, however, would be exceedingly expensive—especially for small- and medium-sized enterprises—and pose numerous technical problems for the global business models of most U.S. companies operating in Europe. Beyond the costs to individual firms, data localization measures can increase cybersecurity and other operational risks and make regulatory compliance and global risk management more difficult. Moreover, in our increasingly digitized economy, embracing data localization in Europe would set a damaging precedent for other countries and could imperil the open, interoperable, secure, and reliable Internet on which our citizens and businesses of all sizes have come to depend so heavily.

Suffice to say, the *Schrems II* ruling also calls into question the ability of European governments to share data with the United States for national security and law enforcement purposes, putting citizens on both sides of the Atlantic at risk. European authorities should recognize that the mere location of data does not ensure information security or privacy, and there are other public policy objectives that are equally important, including financial stability, operational resilience, and innovation—all objectives that depend on cross-border data flows.

U.S. Government Response to Schrems II

While we were deeply disappointed and do not agree with the Court's decision, we are committed to working with our European Commission partners to address the Court's concerns and enable companies to continue to transfer personal data from the EU to the United States. The Administration seeks to ensure the continuity of transatlantic data flows in a manner consistent with U.S. economic and national security interests.

It is important to note that the *Schrems II* ruling focused exclusively on government access to data. The Court did not question the extensive protections Privacy Shield offers EU individuals with respect to the commercial collection and uses of personal data. We believe Privacy Shield already provides strong and predictable protections for EU individuals and any enhancements to the Framework will build on this strong foundation.

As a first step in our efforts to return stability to transatlantic data flows, we engaged with the European Commission to begin working on a solution to Privacy Shield's invalidation. On August 10, Secretary Ross and European Commissioner for

Justice Reynders released a joint statement announcing that the U.S. Department of Commerce and the European Commission had initiated discussions on potential enhancements to Privacy Shield Framework that address the Court's concerns.

Thereafter, in view of the considerable uncertainties concerning the use of SCCs, we worked with our interagency colleagues to bolster companies' ability to utilize the SCCs while we worked to negotiate the necessary enhancements to Privacy Shield. To that end the U.S. Government released a White Paper to assist organizations using SCCs in making the case-by-case assessments called for under *Schrems II* as to whether U.S. law concerning government access to personal data meets EU standards. The White Paper includes a wide range of information about the extensive privacy protections in current U.S. law and practice relating to government access to data for national security purposes—and sets forth clearly the strong and multilayered protections provided under our system. While it is ultimately up to companies to make their own assessments under EU law, the White Paper has, by all accounts, proven to be a useful tool in conducting those assessments.

The objective of any potential agreement between the United States and the European Commission to address *Schrems II* is to restore the continuity of transatlantic data flows and the Framework's privacy protections by negotiating targeted enhancements to Privacy Shield that address the Court's concerns in *Schrems II*. Any such enhancements must respect the U.S. Government's security responsibilities to our citizens and allies.

To be clear, we expect that any enhancements to the Privacy Shield Framework would also cover transfers under all other EU-approved data transfer mechanisms like SCCs and BCRs as well.

The *Schrems II* decision has underscored the need for a broader discussion among likeminded democracies on the issue of government access to data. Especially as a result of the extensive U.S. surveillance reforms since 2015, the United States affords privacy protections relating to national security data access that are equivalent to or greater than those provided by many other democracies in Europe and elsewhere. To minimize future disruptions to data transfers, we have engaged with the European Union and other democratic nations in a multilateral discussion to develop principles based on common practices for addressing how best to reconcile law enforcement and national security needs for data with protection of individual rights.

It is our view that democracies *should* come together to articulate shared principles regarding government access to personal data—to help make clear the distinction between democratic societies that respect civil liberties and the rule of law and authoritarian governments that engage in the unbridled collection of personal data to surveil, manipulate, and control their citizens and other individuals without regard to personal privacy and human rights. Such principles would allow us to work with like-minded partners in preserving and promoting a free and open Internet enabled by the seamless flow of data.

5. CONCLUSION

In closing, the International Trade Administration, the Commerce Department, and the Administration remain committed to restoring clarity and certainty to transatlantic data flows and privacy as quickly as we can. We are hopeful that our European Commission partners share our sense of urgency, and we appreciate the support and attention you and your colleagues here in Congress have brought—and can continue to bring—to the critical issue of cross-border data flows.

Thank you again for this opportunity to appear today.

The CHAIRMAN. Thank you very much. Mr. Phillips.

STATEMENT OF HON. NOAH JOSHUA PHILLIPS, COMMISSIONER, FEDERAL TRADE COMMISSION

Mr. PHILLIPS. Thank you, Mr. Chairman. Chairman Wicker, Ranking Member Cantwell, members of the Committee, thank you for the opportunity to testify before you today. My testimony is my own and does not necessarily reflect the views of other Federal Trade Commissioners or the Commission itself. The *Schrems II* decision and the growth of other impediments to cross-border data flows deserve serious attention. This committee has engaged already and today's hearing is an important continuation of that effort. I thank you.

Mr. Sullivan testified about the terrific work the Administration is doing, and with Presidential transition already underway, your leadership and your support for a path forward are essential. The privacy work of the FTC helps support the free and open Internet. Since the 1990s, we have pursued hundreds of privacy cases, hosted dozens of workshops, and produced many reports relating to privacy and data security. On the Privacy Shield framework and its predecessor specifically, we have brought over 60 cases enforcing commitments that companies make.

I submitted a written statement that I will briefly address the importance of cross-border data flows, the FTC's role in supporting them, impediments they face, and suggestions on moving forward. From small startups to our largest technology companies, connected cars to contact tracing, American companies are competing and winning by offering products and services built on data. Our businesses employ data to support new technologies like artificial intelligence, and as the COVID–19 crisis makes clear, to meet longstanding needs like education, worship, health, and work. Cross-border data flows are an essential component to that. Companies of all sizes, but particularly small businesses, rely on them to reach new customers abroad, to enhance security, and to reduce costs. That means jobs for American workers, and products and services for American consumers.

At FTC, our enforcement approach emphasizes harms with a substantial impact on consumers, permitting both innovation and enforcement. Recent cases include TikTok, before the company was a matter of national conversation, Facebook, YouTube, and just recently Zoom. By any reasonable metric, our enforcement program has had a greater impact than any in the world. We have been a key partner in Privacy Shield and are committed to working with the Department of Commerce to support the free transatlantic flow of data. Today, those flows are at risk.

The European Court of Justice struck down Privacy Shield, expressing concerns about U.S. protections for European data, including redress. The decision also raised questions about standard contractual clauses, the other common legal basis for transfers. That creates legal uncertainty, a cost borne disproportionately by smaller companies, the bulk of Privacy Shield participants. The court's decision concerned National Security and three things strike me as noteworthy. First, U.S. law and practice incorporate substantial civil liberty protections against Government surveillance. Second, the U.S. is at least as protective of privacy as the domestic laws of many of our European allies.

Finally, as Adam Klein, Chairman of the Privacy and Civil Liberties Oversight Board recently noted, European allies regularly partner with the U.S. to assist in their collection of intelligence data. Beyond *Schrems II,* prominent European voices have called for data localization requirements, sometimes under the rubric of data sovereignty. Localization also poses a threat to cross-border data flows.

Historically, we associate it with a kind of State-controlled Internet governance in countries like China. Liberal democracies, which have distinct but fundamentally common approaches to privacy and civil liberties, should be uniting, not splintering. Not only will this

aid U.S. commerce, it will demonstrate a better way for those countries yet to decide on a path for their digital future. So, what can we do? First, we need to find a path to permit transfers between the U.S. and EU.

As exemplified by Jim and his team, this has been a priority for the Administration, and I have every hope and expectation that it will remain one for the incoming Administration, and I ask for your help in ensuring that it is. Second, we must continue to engage with nations evaluating their approach to digital governance to promote the benefits of a free and open Internet. Third, we should vocally defend American values. When it comes to civil liberties and the enforcement of privacy laws, we are second to none. Fourth, as European leaders call to strengthen ties with the U.S., we should prioritize making our regimes interoperable.

Relatively minor differences should not impede mutually beneficial commerce. Finally, any lines should be drawn between allies with shared values and others, like China, which offer a starkly different vision of Internet governance. I thank the Committee for engaging with these challenges and for inviting me, and I look forward to your questions.

[The prepared statement of Mr. Phillips follows:]

PREPARED STATEMENT OF HON. NOAH JOSHUA PHILLIPS,[1] COMMISSIONER, FEDERAL TRADE COMMISSION

Chairman Wicker, Ranking Member Cantwell, Members of the Committee, thank you for the opportunity to testify before you today.

As the agency charged with enforcing the bulk of U.S. privacy law, the Federal Trade Commission supports cross-border data flows through law enforcement, cooperation with the Department of Commerce and other agencies in international engagement, and research and advocacy concerning privacy and data security law and policy. Specifically with respect to the EU–U.S. Privacy Shield Framework ("Privacy Shield") and its predecessor, we have brought over 60 enforcement actions against companies that have failed to live up to their commitments, participated in the Privacy Shield annual review process, and worked with counterpart independent data protection authorities on a host of issues.

A free and open Internet is vital to the national interest, but it is at risk. The impact on U.S. commerce and cross-border data flows from the "*Schrems II*" decision by the European Union Court of Justice ("ECJ"),[2] and the growth of other impediments to that commerce, deserve our serious and immediate attention. This Committee has engaged actively since the ECJ's decision was rendered in August, and today's hearing marks an important, bipartisan, continuation of that effort. With terrific work ongoing by this Administration—about which you will hear today—and a presidential transition underway, your leadership in drawing attention to this issue and your support for a path forward are essential.

My testimony will address the importance of cross-border data flows, the Federal Trade Commission's role in supporting them, the impediments they nonetheless face, and some suggestions on how to move forward.

The Importance of Cross-Border Data Flows

Data help power the U.S. economy. From small startups to our largest technology companies, connected cars to contact tracing, American companies are competing and winning by offering consumers and clients products and services built on data. Our businesses employ data to develop new technologies like artificial intelligence and also to help meet longstanding needs, like education, worship, health, and office work, in novel ways. The COVID–19 crisis makes this abundantly clear.

Cross-border data flows are an essential component enabling all of this. Companies of all sizes rely on these data flows to innovate, reach new customers abroad,

[1] My comments today are my own and do not necessarily reflect the views of the Commission or my fellow Commissioners.

[2] Case C–311/18, *Data Prot. Comm'r v. Facebook Ireland & Maximillian Schrems,* ECLI:EU:C:2020:559 (July 16, 2020) ("*Schrems II*").

improve efficiency, enhance security, and reduce costs,[3] permitting the expansion and innovation that draws investment capital and creates jobs at home. That is particularly true for small companies, which cannot afford to, for example, establish offices or host data centers overseas. Cross-border data flows allow these companies to gain scale more rapidly and compete internationally at lower cost and with less risk. That is doubtless why 65 percent of companies participating in Privacy Shield are small and medium businesses.[4] A 2016 study found that almost two-thirds of worldwide startups surveyed had customers or users in other countries.[5] Take Etsy, the Brooklyn-based custom craft marketplace that offers small businesses a turnkey option to reach a global customer base. In 2019, cross-border transactions made up the largest component of the 36 percent of business attributable to Etsy's international business.[6] Or consider that PayPal—based in San Jose and serving many smaller businesses—has processed over $400 billion in cross border payments since 2003.[7] The list goes on.

The impact of cross-border digital commerce numbers in the trillions of dollars, adding by some estimates hundreds of billions of dollars annually to U.S. GDP.[8] And there is every reason to believe that, if allowed to do so, those numbers will continue to grow. Cross-border data flows are a critical input to our technology sector, in which American companies lead the way. Of technology firms in the Fortune Global 500, the U.S. has 12, nearly double the number of Japan, the next on the list.[9] With our increasingly data-driven economy, cross-border data flows also drive innovation and growth in other sectors as well. At the end of the day, all of that means jobs for American workers and products for consumers.

---

[3] *See, e.g.,* Joshua P. Meltzer & Peter Lovelock, *Regulating for a Digital Economy: Understanding the Importance of Cross-border Data Flows in Asia* 6 (Brookings Inst. Global Econ. & Dev. Working Paper No. 113) (Mar. 20, 2018), *https://www.brookings.edu/wp-content/uploads/2018/03/digital-economy_meltzer_lovelock_web.pdf* (discussing access to new markets and capabilities of "digital inputs such as cloud computing [which] provides on-demand access to computing power and software that was previously reserved for large companies"); ICC Comm'n on Trade & Inv. Pol'y & ICC Comm'n on the Digit. Econ., Int'l Chamber of Com., *Trade in the Digital Economy: A Primer on Global Data Flows for Policymakers* 2 (2016), *https://cdn.iccwbo.org/content/uploads/sites/3/2016/09/Trade-in-the-digital-economy-A-primer-on-global-data-flows-for-policymakers.pdf* ("Access to digital products and services, such as cloud applications, provides SMEs with cutting edge services at competitive prices, enabling them to participate in global supply chains and directly access customers in foreign markets in ways previously only feasible for larger companies. Indeed, the Internet is a great equalizer, enabling small companies to compete globally using the same tools as large and established companies."); Bus. Roundtable, *Putting Data to Work: Maximizing the Value of Information in an Interconnected World* 6 (2015), *https://s3.amazonaws.com/brt.org/archive/reports/BRT%20PuttingDataToWork.pdf* (discussing how Caterpillar uses sensor data to allow it "and its customers to remotely monitor assets across their fleets in real time"); Demetrios Marantis, *Cross-border data flows power small business recovery,* Visa, Inc. (Nov. 9, 2020), *https://usa.visa.com/visa-everywhere/blog/bdp/2020/11/09/cross-border-data-flows-1604955432332.html* (noting that cross-border data flows are used to improve AI the provides fraud detection).

[4] Oliver Patel & Dr. Nathan Lea, UCL Eur. Inst, *EU-U.S. Privacy Shield, Brexit and the Future of Transatlantic Data Flows* 12 (May 2020), *https://www.ucl.ac.uk/european-institute/sites/european-institute/files/privacy_shield_brexit_and_the_future_of_transatlantic_data_flows_1.pdf.*

[5] James Manyika & Susan Lund, *Digital Protectionism and Barriers to International Data Flows,* Bretton Woods Comm. (Jun. 25, 2018), *https://www.brettonwoods.org/article/digital-protectionism-and-barriers-to-international-data-flows.*

[6] Etsy, Inc., Annual Report (Form 10–K) 66 (Feb. 27, 2020), *https://d18rn0p25nwr6d.cloudfront.net/CIK-0001370637/d63aa848-ac0c-474c-9350-5b18888e84bf.pdf.* International business includes all transactions "where either the billing address for the seller or the shipping address for the buyer at the time of sale is outside of the United States." *Id.*

[7] Peggy Abkemeier, *Cross-Border Trade: PayPal's $400B Business,* PayPal Holdings, Inc. (Apr. 6, 2017), *https://www.paypal.com/stories/us/cross-border-trade-paypals-400b-business.*

[8] James Manyika *et al.,* McKinsey & Co., *Digital Globalization: The New Era of Global Flows* 10 (Feb. 24, 2016), *https://www.mckinsey.com/~/media/McKinsey/Business%20Functions/McKinsey%20Digital/Our%20Insights/Digital%20globalization%20The%20new%20era%20of%20global%20flows/MGI-Digital-globalization-Full-report.pdf* (estimating impact on global GDP of $2.8 trillion in 2014); Gary Clyde Hufbauer & Zhiyao (Lucy) Lu, *Can Digital Flows Compensate for Lethargic Trade and Investment?,* Petersen Inst. for Int'l Econ. (Nov. 28, 2018), *https://www.piie.com/blogs/trade-investment-policy-watch/can-digital-flows-compensate-lethargic-trade-and-investment* (estimating impact on global GDP of over $3.5 trillion in 2020); U.S. Int'l Trade Comm'n, No. 4485, *Digital Trade in the U.S. and Global Economies, Part 2,* at 13 (Aug. 2014), *https://www.usitc.gov/publications/332/pub4485.pdf* (estimating 2011 impact on U.S. GDP of over $500 billion).

[9] *Fortune Global 500,* Fortune (2020), *https://fortune.com/global500/.*

Role of the FTC

The Federal Trade Commission plays an important role in supporting the promise of the free and open Internet, including cross-border data flows.

With respect to data privacy and security, we help ensure that companies communicate honestly with their customers about their privacy and security practices and refrain from unfair privacy or security practices.

Since the enactment of the Fair Credit Reporting Act ("FCRA") in 1970,[10] the FTC has served as the primary Federal agency protecting consumer privacy. With the development of the Internet as a commercial medium in the 1990s, the Commission expanded its focus on privacy to reflect the growing collection, use, and sharing of consumer data in the commercial marketplace. The Commission's main source of legal authority in the privacy and data security space is Section 5 of the FTC Act, which prohibits deceptive or unfair commercial practices.[11] Under Section 5 and other statutes such as the Gramm-Leach-Bliley Act,[12] the Children's Online Privacy Protection Act,[13] and the FCRA, the FTC has aggressively pursued cases in children's privacy, financial privacy, health privacy, the Internet of Things, and beyond. In total, we have brought hundreds of data security and privacy cases and we have hosted about 75 workshops and issued approximately 50 reports in the privacy and security area, on topics from data brokers[14] to portability.[15]

Our approach emphasizes addressing harms that have a tangible, substantial impact on consumers' well-being. This allows for both innovation and enforcement. There are scores of Data Protection Authorities in nations around the world, but no agency has engaged in more, or more significant, privacy and data security enforcement than the FTC. In just the few years of my tenure and those of my fellow commissioners, we have finalized settlements with Facebook[16] and Google/YouTube[17] that mandated both substantial monetary relief and significant improvements in privacy governance practices. In early 2019, we resolved a case against TikTok, long before the company was a matter of national conversation.[18] And, just a few weeks ago, we settled a case against Zoom, including allegations regarding representations the company made about the security of stored and transferred data.[19] In my view, by any reasonable metric, our enforcement program has had a greater impact than any other in the world.

The Commission has played an important role in Privacy Shield[20] and its predecessor, the U.S.-EU Safe Harbor Framework ("Safe Harbor").[21] Under the EU's General Data Protection Regulation ("GDPR") and its predecessors, companies are required to meet certain data protection requirements in order to transfer consumer

---

[10] Fair Credit Reporting Act, 15 U.S.C. § 1681 *et seq.*

[11] 15 U.S.C. § 45.

[12] Gramm-Leach-Bliley Act, Pub. L. No. 106–102, 113 Stat. 1338 (1999) (codified as amended in scattered sections of 12 and 15 U.S.C.); Standards for Safeguarding Customer Information, 16 C.F.R. § 314.

[13] Children's Online Privacy Protection Act, 15 U.S.C. §§ 6501–6506; Children's Online Privacy Protection Rule, 16 C.F.R. § 312.

[14] *See* FTC Report, *Data Brokers: A Call for Transparency and Accountability* (May 2014), *https://www.ftc.gov/system/files/documents/reports/data-brokers-call-transparency-accountability-report-federal-trade-commission-may-2014/140527databrokerreport.pdf.*

[15] *See* FTC Workshop, *Data To Go: An FTC Workshop on Data Portability* (Sept. 22, 2020), *https://www.ftc.gov/news-events/events-calendar/data-go-ftc-workshop-data-portability.*

[16] *See* FTC Press Release, *FTC Imposes $5 Billion Penalty and Sweeping New Privacy Restrictions on Facebook* (July 24, 2019), *https://www.ftc.gov/news-events/press-releases/2019/07/ftc-imposes-5-billion-penalty-sweeping-new-privacy-restrictions.*

[17] *See* FTC Press Release, *Google and YouTube Will Pay Record $170 Million for Alleged Violations of Children's Privacy Law* (Sept. 4, 2019), *https://www.ftc.gov/news-events/press-releases/2019/09/google-youtube-will-pay-record-170-million-alleged-violations.*

[18] *See* FTC Press Release, *Video Social Networking App Musically Agrees to Settle FTC Allegations That it Violated Children's Privacy Law* (Feb. 27, 2019), *https://www.ftc.gov/news-events/press-releases/2019/02/video-social-networking-app-musically-agrees-settle-ftc.*

[19] *See* FTC Press Release, *FTC Requires Zoom to Enhance its Security Practices as Part of Settlement* (Nov. 9, 2020), *https://www.ftc.gov/news-events/press-releases/2020/11/ftc-requires-zoom-enhance-its-security-practices-part-settlement.*

[20] *See* FTC Business Guidance, *Privacy Shield* (2020), *https://www.ftc.gov/tips-advice/business-center/privacy-and-security/privacy-shield.* While I focus here on the U.S.-EU agreements, there was previously a U.S.-Swiss version of Safe Harbor that was replaced by a U.S.-Swiss version of Privacy Shield. The Swiss data protection authorities recently reached a similar decision as the court in *Schrems II.* Mark Smith, *ANALYSIS: Swiss-U.S. Privacy Shield Suffers from Schrems, Too,* Bloomberg L. (Sept. 10, 2020), *https://news.bloomberglaw.com/bloomberg-law-analysis/analysis-swiss-u-s-privacy-shield-suffers-from-schrems-too.*

[21] *See* FTC Business Guidance, *Federal Trade Commission Enforcement of the U.S.-EU and U.S.-Swiss Safe Harbor Frameworks* (2016), *https://www.ftc.gov/tips-advice/business-center/guidance/federal-trade-commission-enforcement-us-eu-us-swiss-safe-harbor.*

data from the EU to other jurisdictions.[22] Privacy Shield and Safe Harbor are voluntary mechanisms ensuring compliance with European requirements that have provided legal bases for companies to transfer data from Europe to the United States.[23]

The FTC can bring enforcement actions against companies that misrepresent their participation in or compliance with Privacy Shield. We have brought over 60 cases enforcing companies' commitments under Safe Harbor and Privacy Shield. We also fill a similar role with the APEC Cross-Border Privacy Rules system, designed to protect privacy and data flows in the Asia-Pacific region.[24]

Even though the court declared the Privacy Shield invalid, which I discuss below, the FTC continues to expect companies to comply with their ongoing obligations with respect to transfers made under Privacy Shield. If companies do not keep their promises, we will enforce the law against them. We also encourage companies to continue to follow robust privacy principles, such as those underlying Privacy Shield, and to review their privacy policies to ensure they describe their privacy practices accurately, including with regard to cross-border data transfers. The Commission remains committed to working with the Department of Commerce to help support the free flow of data across borders.

Schrems II

Notwithstanding these efforts, the privacy protections U.S. law provides U.S. citizens and non-citizens, and the tremendous work this Administration and the prior one have done with their counterparts on the European Commission (the Executive Branch of the EU), transatlantic data flows are threatened.

In 2016, the European Commission deemed Privacy Shield "adequate", thus permitting transfers to the U.S. under the framework.[25] In its recent ruling in *Schrems II,* the ECJ struck down Privacy Shield. The court expressed concerns about U.S. protections described in the European Commission's Privacy Shield Adequacy Decision, including the independence of the Ombudsman mechanism established in the U.S. Department of State and the perceived lack of redress for EU data subjects.[26] Additionally, the court required companies that rely on Standard Contractual Clauses ("SCCs") to assess the level of protection in the importing country for all of their transfers, raising questions about SCCs as a legal basis for transfers to the U.S.[27]

The *Schrems II* decision and recent recommendations from the European Data Protection Board,[28] the coordinating body of local data protection authorities under the GDPR, create substantial legal uncertainty and risk for cross-border data transfers. Those costs are borne disproportionately by small companies, which cannot afford the more expensive options, and for that reason constitute the bulk of companies that participate in Privacy Shield.

The court's decision concerned national security access to personal data, not consumer privacy in the sense that we enforce at the FTC. Meaning, what was at issue in *Schrems II* was not the absence of a GDPR-like national consumer privacy law in the U.S.

Looking at how the court considered U.S. national security access to personal data, three things strike me. *First,* U.S. law and practice incorporate civil liberty protections against government surveillance that are substantial, including statutes

---

[22] Regulation (EU) 2016/679 of the European Parliament and of the Council, Art. 45, General Data Protection Regulation, 2016 O.J. (L 119) 1, 41.

[23] Privacy Shield is not the only mechanism for transferring data to the U.S. from the EU. As discussed below, GDPR permits transfers made using Standard Contractual Clauses and Binding Corporate Rules.

[24] *See* FTC Press Release, *FTC Becomes First Enforcement Authority in APEC Cross-Border Privacy Rules System* (July 26, 2012), *https://www.ftc.gov/news-events/press-releases/2012/07/ftc-becomes-first-enforcement-authority-apec-cross-border-privacy.*

[25] Eur. Comm'n, *Commercial Sector: EU-US Privacy Shield, https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/eu-us-data-transfers_en#:~:text=The%20adequacy%20decision%20on%20the,United%20States%20for%20commercial%20purposes.*

[26] *Schrems II, supra* note 2, ¶¶ 186–198.

[27] *Schrems II, supra* note 2, ¶ 142. To be sure, it is the view of many, including the Commerce Department, that SCCs are still available, at least for some transfers. But even where SCCs may still be available, the complexity and risk of using them has increased. *See* Dep't of Com. *et al., Information on U.S. Privacy Safeguards Relevant to SCCs and Other EU Legal Bases for EU-U.S. Data Transfers after Schrems II* (Sept. 2020), *https://www.commerce.gov/sites/default/files/2020-09/SCCsWhitePaperFORMATTEDFINAL508COMPLIANT.PDF.*

[28] Eur. Data Prot. Bd., *Recommendations 01/2020 on Measures That Supplement Transfer Tools to Ensure Compliance with the EU Level of Protection of Personal Data* (Nov. 10, 2020), *https://edpb.europa.eu/sites/edpb/files/consultation/edpb_recommendations_202001_supplementarymeasurestransferstools_en.pdf.*

such as the Electronic Communications Privacy Act[29] and the Judicial Redress Act[30] and executive actions like Presidential Policy Directive 28.[31] *Second,* as researchers in the U.S. and Europe have found, U.S. law and practice are *at least* as protective of privacy as the domestic laws of many of our European allies.[32] The court, however, deemed European domestic laws irrelevant, focusing instead on what Professor Peter Swire has referred to as "an idealized, formal standard set forth primarily in EU constitutional law", rather than the national security laws and practices of members states.[33] *Finally,* as Adam Klein, Chairman of the Privacy and Civil Liberties Oversight Board recently noted, those allies regularly partner with the U.S. to assist in their collection of valuable intelligence data.[34]

Schrems II is not the only risk factor for cross-border data flows. Both before and since the decision, sometimes under the rubric of "data sovereignty", a number of prominent European voices[35] have called for data localization requirements in Europe—that is, for all data about Europeans to be kept in Europe.

By no means are data localization concerns unique to Europe. By some estimates, localization efforts have grown fourfold since 2000, including many sector-specific rules requiring that certain data be processed or maintained in-country.[36] Countries that have, or are considering, localization requirements include India, Vietnam, Australia, and Turkey.[37]

Adopting data localization around the world poses a threat to U.S. commerce as well as the free and open Internet. To do business in multiple countries, companies will need servers, local staff, and so on. For smaller companies and startups, this may spell the end of cross-border commerce. The result will negatively impact not only American companies looking to grow but American consumers who benefit from products improved by cross-border data flows.

For larger firms that can add processing capacity overseas, there still are downsides. For instance, localization inhibits the global backup and redundancy that a distributed network allows, and the privacy and security that come with it.[38] Even something as uncontroversial as bug and error reporting from individual computers—which allows companies to analyze and correct software issues—may be-

---

[29] Electronic Communications Privacy Act of 1986, Pub. L. No. 99–508, 100 Stat. 1848 (codified as amended in scattered sections of 18 U.S.C.).

[30] Judicial Redress Act, 5 U.S.C. § 552a note.

[31] Presidential Policy Directive 28—Signals Intelligence Activities, 1 Pub. Papers 46 (Jan. 17, 2014), *https://www.govinfo.gov/content/pkg/PPP-2014-book1/pdf/PPP-2014-book1-doc-pg46.pdf.*

[32] *See, e.g.,* Jacques Bourgeois *et al.,* Sidley Austin LLP, *Essentially Equivalent: A Comparison of the Legal Orders for Privacy and Data Protection in the European Union and United States,* at iv (Jan. 2016), *https://www.sidley.com/-/media/publications/essentially-equivalent-final.pdf* (arguing that "the U.S. legal order for privacy and data protection embodies fundamental rights consistent with the Charter, principles of proportionality, and checks and balances in both form and substance, and that these protections of privacy and data protection rights are essentially equivalent to those in the EU").

[33] Kenneth Propp & Peter Swire, *Geopolitical Implications of the European Court's Schrems II Decision,* Lawfare (July 17, 2020), *https://www.lawfareblog.com/geopolitical-implications-european-courts-schrems-ii-decision.*

[34] Adam Klein, Chairman, Priv. & C.L. Oversight Bd., Statement on the Terrorist Finance Tracking Program (Nov. 19, 2020), *https://documents.pclob.gov/prod/Documents/EventsAndPress/b8ce341a-71d5-4cdd-a101-219454bfa459/TFTP%20Chairman%20Statement%2011_19_20.pdf.*

[35] *See, e.g.,* Vincent Manancourt, *Europe's data grab,* Politico (Feb. 12, 2020), *https://www.politico.eu/article/europe-data-grab-protection-privacy/;* Thierry Breton, Comm'r, *Europe: The Keys To Sovereignty,* Eur. Comm'n (Sept. 11, 2020), *https://ec.europa.eu/commission/commissioners/2019-2024/breton/announcements/europe-keys-sovereignty_en.*

[36] Christian Ketels & Arindam Bhattacharya, *Global Trade Goes Digital,* Bos. Consulting Grp. (Aug. 12, 2019), *https://www.bcg.com/publications/2019/global-trade-goes-digital;* Jennifer Huddleston & Jacqueline Varas, *Impact of Data Localization Requirements on Commerce and Innovation,* Am. Action F. (June 16, 2020), *https://www.americanactionforum.org/insight/impact-of-data-localization-requirements-on-commerce-and-innovation/#ixzz6YgQOlW4C* ("The data covered by these laws can range from all personal data to only specific types of data such as health or financial information.").

[37] Pablo Urbiola *et al.,* Inst. of Int'l Fin., *Data Flows Across Borders: Overcoming Data Localization Restrictions* 1, 2 (Mar. 2019), *https://www.iif.com/Portals/0/Files/32370132_iif_data_flows_across_borders_march2019.pdf;* David Meyer, *Here's Why PayPal Is About to Suspend Operations in Turkey,* Fortune (May 31, 2016), *https://fortune.com/2016/05/31/paypal-turkey-suspension/.*

[38] For example, data may be divided into shards, with any individual's data split up across multiple machines across the world. H Jacqueline Brehmer, *Data Localization: The Unintended Consequences of Privacy Litigation,* 67 Am. U. L. Rev. 927, 967–986 (2018), *https://digitalcommons.wcl.american.edu/cgi/viewcontent.cgi?article=2009&context=aulr;* Dillon Reisman, *Where Is Your Data, Really?: The Technical Case Against Data Localization,* Lawfare (May 22, 2017), *https://www.lawfareblog.com/where-your-data-really-technical-case-against-data-localization.*

come a local function deprived of critical inputs. And research institutions will feel the impact, with cross-border collaboration in areas like medicine and computer science—where access to large and global data sets are essential—newly subject to digital boundaries.[39]

Data localization requirements are nothing new but historically have more often been associated with alternative visions of Internet governance in countries like China and Russia. The hallmark of this alternative is state control: the opposite of a free and open Internet. China uses technical controls (its "great firewall") and legal controls to filter what is available to Chinese citizens.[40] There is active censorship at the national level, such that you can't type Winnie the Pooh—a reference used by critics of President Xi—into Weibo without it being deleted.[41] And, not surprisingly, China also requires that substantial amounts of data be stored on servers in China.[42] Data stored locally are accessible to the government upon request, and without due process.[43]

Russia also maintains strict data localization laws (though not always enforced);[44] allows for blacklisting of Internet sites;[45] and has experimented with creating, in effect, its own internet, with exclusively in-country routing, DNS, and the like.[46]

Let me stress that the liberal democracies of Europe are nothing like China and Russia, but impeding cross-border data flows and erecting unnecessary barriers—the "Splinternet", as Stanford Law Professor Mark Lemley refers to it in a recent article[47]—will reverberate. In many parts of the world, including nations with which the U.S. does substantial commerce, which path to follow remains an open question. Liberal democracies should be uniting—not dividing—to light the better path.

---

[39] *See, e.g.,* PHG Found., *Impact of Schrems II on Genomic Data Sharing* (2020), *https://www.phgfoundation.org/documents/schrems-ii-discussion-paper.pdf* (noting how *Schrems II* impacts genomic research).

[40] Elizabeth C. Economy, *The great firewall of China: Xi Jinping's Internet shutdown,* Guardian (June 29, 2018), *https://www.theguardian.com/news/2018/jun/29/the-great-firewall-of-china-xi-jinpings-internet-shutdown.*

[41] Yuan Yang, *Winnie the Pooh blacklisted by China's online censors,* Fin. Times (July 16, 2017), *https://www.ft.com/content/cf7fd22e-69d5-11e7-bfeb-33fe0c5b7eaa.*

[42] Yuxi Wei, *Chinese Data Localization Law: Comprehensive but Ambiguous,* Henry M. Jackson Sch. of Int'l Stud., Univ. of Wash. (Feb. 7, 2018), *https://jsis.washington.edu/news/chinese-data-localization-law-comprehensive-ambiguous/* (localization requirements in China are comprehensive but also confusing and ambiguous).

[43] Afef Abrougi, *Chinese law and state security requirements stunt companies' progress in 2019 RDR Index,* Ranking Digit. Rts. (July 17, 2019), *https://rankingdigitalrights.org/2019/07/17/chinese-law-and-state-security-requirements-stunt-companies-progress-in-2019-rdr-index/* (Chinese law requires "to keep user activity logs and relevant data for six months and to hand it over to the authorities when requested without due process"); Martina F. Ferracane & Hosuk Lee-Makiyama, Eur. Ctr. For Int'l Pol. Econ., *China's Technology Protectionism and its Non-negotiable Rationales* 3 (June 2017), *https://ecipe.org/wp-content/uploads/2017/06/DTE_China_TWP_REVIEWED.pdf* ("[T]he State Security Law (passed in 1993) provides the state security organs with access to any information or data held by an entity in China whenever they deem it necessary. Without doubt, the scope of the State Security Law has grown exponentially in the digitalisation era."); Adrian Shahbaz, Freedom House, *The Rise of Digital Authoritarianism* (2018), *https://freedomhouse.org/report/freedom-net/2018/rise-digital-authoritarianism* ("China was once again the worst abuser of Internet freedom in 2018.").

[44] Vera Shaftan, *Russian Data Localization law: now with monetary penalties,* Data Prot. Rep. (Dec. 20, 2019), *https://www.dataprotectionreport.com/2019/12/russian-data-localization-law-now-with-monetary-penalties/#:~:text=By%20way%20of%20recap%2C%20in,using%20databases%20located%20in%20Russia* ("[I]n 2015, Russia introduced a data localization law, requiring "data operators" to ensure that recording, systematisation, accumulation, storage, refinement and extraction of personal data of Russian citizens is done using databases located in Russia.").

[45] Freedom House, *Freedom on the Net 2019, Russia* (2019), *https://freedomhouse.org/country/russia/freedom-net/2019* ("The government gives several state bodies—including Roskomnadzor, the Prosecutor General's Office, the Federal Service for Surveillance on Consumer Rights Protection and Human Wellbeing (Rospotrebnadzor), the Federal Drug Control Service, and, most recently, the Federal Agency for Youth Affairs—the authority to block various categories of online content.").

[46] Isabelle Khurshudyan, *Russia is bolstering its Internet censorship powers—is it turning into China?,* Independent (Feb. 3, 2020), *https://www.independent.co.uk/news/world/europe/russia-internet-censorship-norway-putin-a9306666.html* (observing that a 2019 law "aims to route Russian web traffic and data through points controlled by state authorities and to build a national domain name system. This, supporters claim, would give Russia greater control of Internet content and traffic.").

[47] Mark A. Lemley, *The Splinternet* (Stan. Law & Econ. Olin Working Paper No. 555, 2020), *http://dx.doi.org/10.2139/ssrn.3664027.* Professor Lemley is not the first to use this term.

Next Steps

All of this demonstrates the need to foster transatlantic data flows, and international ones more broadly.

First, we need to find a path forward after *Schrems II,* to permit transfers between the U.S. and EU. I want to recognize the efforts of U.S. and EU negotiators to find a replacement for Privacy Shield. While no doubt challenging, I have confidence in the good faith and commitment of public servants like Jim Sullivan, with whom I have the honor of appearing today, and our partners across the Atlantic. I have every hope and expectation that protecting cross-border data flows will be a priority for the incoming Administration, and I ask for your help in ensuring it is.

Second, we must actively engage with nations evaluating their approach to digital governance, something we at the FTC have done, to share and promote the benefits of a free and open Internet. There is an active conversation ongoing internationally, and at every opportunity—whether in public forums or via private assistance—we must ensure our voice and view is heard.

Third, we should be vocal in our defense of American values and policies. While we as Americans always look to improve our laws—and I commend the members of this committee on their important work on privacy legislation and other critical matters—we do not need to apologize to the world. When it comes to civil liberties or the enforcement of privacy laws, we are second to none. Indeed, in my view, the overall U.S. privacy framework—especially with the additional protections built into Privacy Shield—should certainly qualify as adequate under EU standards.

Fourth, as European leaders call to strengthen ties with the U.S., we should prioritize making our regimes compatible for the free flow of data. This extends to the data governance regimes of like-minded countries outside of Europe as well. Different nations will have different rules, but relatively minor differences need not impede mutually-beneficial commerce.[48] We need not and should not purport to aim for a single, identical system of data governance. And we should remind our allies, and remind ourselves, that far more unites liberal democracies than divides us.[49]

Fifth and finally, if we must draw lines, those lines should be drawn between allies with shared values—the U.S., Europe, Japan, Australia, and others—and those, like China and Russia, that offer a starkly different vision. I am certainly encouraged when I hear recognition of this distinction from Europe. European Data Protection Supervisor Wojciech Wiewiórowski recently noted that the U.S. is much closer to Europe than is China and that he has a preference for data being processed by countries that share values with Europe.[50] Some here in the U.S. are even proposing agreements to solidify the relationships among technologically advanced democracies, an idea worth exploring in more detail.[51]

However we proceed will require vision and leadership, and that is why I am so glad that this committee is prepared to engage thoughtfully with these challenges.

Again, thank you for inviting me today, and I look forward to your questions.

The CHAIRMAN. Thank you very much. Ms. Espinel, you are recognized.

---

[48] *See, e.g.,* Remarks of Jennifer Daskal, *Debate: We Need to Protect Strong National Borders on The Internet,* 17 Colo. Tech. L.J., 13, 27 ("[T]he goal is to figure out a way to mediate, and manage, those differences, without yielding a fractured Internet.").

[49] For one model of how to bridge the divide, consider the CLOUD Act, which provides for U.S. law enforcement access to data stored overseas while recognizing and respecting the citizens and laws of the hosting country. *See, e.g.,* Alan Charles Raul, *Global Overview,* Privacy, Data Prot. and Cybersecurity L. Rev., 1, 2 (Alan Charles Raul ed., 2020), *https://www.sidley.com/-/media/publications/the-privacy-data-protection-and-cybersecurity-law-review-2020-global-overview.pdf?la=en;* Daskal, *supra* note 48, at 29.

[50] Peter Swire, *'Schrems II' backs the European legal regime into a corner—How can it get out?,* IAPP (July 16, 2020), *https://iapp.org/news/a/schrems-ii-backs-the-european-legal-regime-into-a-corner-how-can-it-get-out/.*

[51] *See, e.g.,* Robert K. Knake, Council on Foreign Rels., *Weaponizing Digital Trade: Creating a Digital Trade Zone to Promote Online Freedom and Cybersecurity* (Sept. 2020), *https://cdn.cfr.org/sites/default/files/report_pdf/weaponizing-digital-trade_csr_combined_final.pdf;* Jared Cohen & Richard Fontaine, *Uniting the Techno-Democracies,* Foreign Affs., Nov.–Dec. 2020, *https://www.foreignaffairs.com/articles/united-states/2020-10-13/uniting-techno-democracies* (suggesting an informal group of technologically advanced states which would hold regular meetings).

STATEMENT OF VICTORIA A. ESPINEL, PRESIDENT AND CHIEF EXECUTIVE OFFICER, BSA | THE SOFTWARE ALLIANCE

Ms. ESPINEL. Good morning—and members of the Committee. My name is Victoria Espinel and I am President and CEO of BSA | the Software Alliance. Data flows are not often the topic of headlines or congressional hearings, even though they are integral to our daily lives. That is because when they are permitted and when the data is kept private, our expectations as consumers are met and our businesses can operate effectively. However, if they are disrupted, we all face problems.

I commend the Committee for holding this hearing on the critical issue of cross-border data transfers and for the opportunity to testify here today. Today's consumers and businesses of all sizes and in all industries expect services that offer privacy and security. Those services often require connecting people who sit on different sides of the globe, yet need access to the same data. And that requires moving data between countries and across legal systems.

As individuals, we rely on data transfers in our jobs and lives every day without even thinking about it. It might be the H.R. system that ensures you are paid on time. It might be your company's e-mail contacts that includes colleagues that are abroad. It might be your credit card which checks for and stops fraudulent transactions. Data transfers are foundational to any business with employees, customers, vendors, or locations outside the United States. For example, farmers use global data to understand weather patterns and soil conditions around the world to increase their crop yields and lower their cost. Similarly, manufacturers use data from factory floors across the world to monitor the safety and performance of their machines. It is difficult to overstate the importance of cross-border data transfers to U.S. consumers, U.S. businesses of all sizes and sectors, and the entire U.S. economy, particularly in light of COVID.

The crosscutting importance of this issue led BSA to launch a new initiative earlier this year, the Global Data Alliance, that brings together companies and a range of industries who are united by the importance of transferring data across borders in a manner that strongly protects personal privacy. At BSA, we represent the enterprise software perspective and our members create the technology that other businesses use. Those businesses trust BSA members to maintain the privacy and security of their most sensitive data, and our companies work hard to earn that trust. I want to emphasize that there should be no tradeoff between the need to transfer data and the need to protect the privacy of that data. Both are essential. In our view, personal data should only be transferred or used in any way with real effective privacy protections.

BSA also supports strong privacy legislation. I was honored to testify before this committee at the beginning of this Congress on privacy legislation. And I want to thank Chairman Wicker, Ranking Member Cantwell, and Senators Moran, Blumenthal, Thune, Schatz, Markey, Klobuchar and others for their hard work and leadership to develop concrete proposals that will form the basis for passing privacy legislation next year. While I have focused on the ability to send data across borders in general, today's hearing fo-

cuses on the specific and importance of transfers, those between the United States and the European Union.

The EU requires transferring personal data use a transfer mechanism. The U.S.-EU Privacy Shield was for many years a trusted way to do this. When the Privacy Shield and other transfer mechanisms were challenged in the European court, BSA participated as an amicus alongside the U.S. Government and the European Commission. This July, the Court of Justice of the European Union invalidated the Privacy Shield in its so-called *Schrems II* decision that had an immediate impact on 5,300, mostly small and medium sized businesses that relied on the Privacy Shield.

I want to emphasize that the decision did not question the privacy practices of the companies participating in the Privacy Shield. The court also upheld the use of standard contractual clauses, which will become even stronger when a new U.S.-EU agreement is reached. We applaud the quick response by policymakers on both sides of the Atlantic. I want to thank Mr. Sullivan and Commissioner Philips for their immediate response. We particularly appreciate the leadership efforts by this committee and the strong, bipartisan, bicameral support. Chairman Wicker, Ranking Member Cantwell, thank you for the letter that you and your House counterparts sent to the FTC and Commerce shortly after the court's decision.

In addition to these urgent near-term efforts, I want to encourage this committee to think boldly about longer term, sustainable ways to address the underlying intelligence gathering issues, and to work toward building consensus among like-minded countries. We all realize that some amount of signals intelligence is necessary in a democratic society to ensure safety and security.

The question is, what guardrails and safeguards are needed? Building mutual recognition around these issues is vital over the long term. BSA stands ready to work with the Committee on promoting reliable and secure mechanisms for international data transfers. And I look forward to your questions.

[The prepared statement of Ms. Espinel follows:]

PREPARED STATEMENT OF VICTORIA A. ESPINEL, PRESIDENT AND CEO, BSA | THE SOFTWARE ALLIANCE

Good morning Chairman Wicker, Ranking Member Cantwell, and members of the Committee. My name is Victoria A. Espinel. I am President and CEO of BSA| The Software Alliance ("BSA").

BSA is the leading advocate for the global software industry.[1] Our members are at the forefront of developing cutting-edge, data-driven services that have a significant impact on U.S. job creation and growing the global economy. I commend the Committee for holding this hearing on the important topic of transatlantic data transfers and the EU–US Privacy Shield Framework ("Privacy Shield"), and I thank you for the opportunity to testify.

[1] BSA | The Software Alliance (www.bsa.org) is the leading advocate for the global software industry before governments and in the international marketplace. Its members are among the world's most innovative companies, creating software solutions that spark the economy and improve modern life. With headquarters in Washington, DC, and operations in more than 30 countries, BSA pioneers compliance programs that promote legal software use and advocates for public policies that foster technology innovation and drive growth in the digital economy. BSA's members include: Adobe, Atlassian, Autodesk, Bentley Systems, Box, Cadence, CNC/Mastercam, DocuSign, IBM, Informatica, Intel, MathWorks, Microsoft, Okta, Oracle, PTC, Salesforce, ServiceNow, Siemens Industry Software Inc., Sitecore, Slack, Splunk, Trend Micro, Trimble Solutions Corporation, Twilio, and Workday.

Cross-border data transfers are critical to the success of a broad range of companies, of all sizes and industries, and to consumers on both sides of the Atlantic. For that reason, the issues before this Committee reach far beyond the technology sector. Companies large and small, across the entire U.S. economy, depend on services that send data across international borders.

BSA represents the perspective of enterprise software companies. Our members create the technology products and services that help other businesses innovate and grow. Businesses trust BSA members to maintain the privacy and security of their most sensitive data, including personal information. Those businesses—in sectors as diverse as agriculture, healthcare, manufacturing, and banking—produce a broad range of products and services and are united by the need to send data across international borders. Indeed, everyday technologies like cloud storage services, customer relationship management software, human resource management programs, identity management services, workplace collaboration software, and supply chain management services all depend on the ability to transfer data across national boundaries.

Transferring data across borders is not only vital to businesses, but also to consumers and workers. In our professional lives, we transfer data when we send emails to colleagues, manage staff and budgets, attend videoconferences, and in thousands of other routine business activities. In our personal lives, we transfer data across borders when we engage in e-commerce or use messaging platforms to stay in touch with friends and relatives overseas. In each of these scenarios, we rightly expect to use global services that can connect us with others worldwide—in a manner that protects the privacy and security of our data.

These issues are even more important amid the COVID–19 pandemic, as companies across the economy rely more heavily on remote workplace tools and cloud-based technologies that help employees remain productive while working outside of their physical offices. Online tools are also opening new avenues for medical researchers, hospitals, and pharmaceutical companies to coordinate research and treatment efforts, and for regulators to more quickly and accurately assess potential vaccines and treatments. Small businesses are increasingly serving customers not only in physical stores but also through online models that let them reach customers worldwide. As individuals, we are also shifting our lives even further online—whether it is to buy goods and services or to gather with relatives and friends.

In short, it is difficult to overstate the importance of cross-border data transfers to U.S. consumers, businesses of all sizes and sectors, and the entire economy. That is why I want to focus my testimony on the need to ensure companies can continue transferring data across international borders, so they can provide the products and services their customers demand, in a way that respects the privacy and security of the transferred data.

Today's hearing focuses on the Privacy Shield, which until recently served as a privacy-protective way for companies to transfer data from the EU to the United States, consistent with EU legal requirements and privacy expectations of EU and U.S. citizens. The Privacy Shield was invalidated in July, when the Court of Justice of the European Union ("CJEU") issued its decision in *Schrems II*. We applaud the swift response to that decision by policymakers on both sides of the Atlantic and their shared recognition that a new agreement is needed to replace the Privacy Shield. In particular, I would like to thank Chairman Wicker and Ranking Member Cantwell for leading a bipartisan and bicameral letter shortly after the Court's decision. Your efforts helpfully demonstrated strong congressional support for the Administration to negotiate with the European Commission to ensure data flows are not unduly disrupted. We welcome this Committee's efforts to continue supporting the important work of developing a successor to the Privacy Shield, to provide a responsible way for companies to transfer data across the Atlantic. At the same time, along with these important near-term efforts, we also encourage the Committee to think boldly about longer-term, sustainable ways to address the underlying issues about intelligence gathering and privacy—and to work toward building consensus on those issues among like-minded countries.

The Ability to Send Data Across International Borders is Critical to Consumers and Companies Worldwide

International data transfers are an essential part of modern-day commerce. They underpin a wide range of everyday business activities. For instance, when an employee joins a video conference with an overseas customer, shares documents with colleagues in a foreign office, sends an order to a supplier in another country, or simply communicates online with someone overseas, that person invariably engages in the cross-border transfer of data. As just one example, modern IT support offered on a 24-hour/7-days-a-week basis—which became critical for many companies even before the current pandemic—would be impossible without the ability to transfer

data across borders. Robust cybersecurity likewise relies on sharing data to help companies quickly identify and respond to threats that, by their nature, do not respect national borders. Indeed, sharing information on how bad actors in one country attempted to breach a system can help companies in other countries thwart similar efforts.

International data transfers are an essential component of products and services across industries. For example:

- *Detecting fraud.* Cross-border data flows help stop credit card fraud on a global scale. By efficiently transmitting data across borders, banks can detect and block fraud attempts in a matter of seconds, regardless of where a purchase is attempted. This process has prevented billions of dollars in losses to online fraudsters.
- *Healthcare.* Cross-border data transfers allow healthcare facilities to make treatments more effective by using clinical support software that analyzes electronic medical records, insurance claims, and datasets across a large and diverse sample size. It can also enable digitized medical images to be shared with non-local specialists for consultations anywhere in the world, improving the quality of medical care regardless of where a patient lives.
- *E-commerce.* Cross-border data flows are at the heart of e-commerce. Retailers send data across borders when they check inventory in an overseas warehouse, accept and process customer orders, and enable customers to track shipments en route to their destination.
- *Human resources management.* Global companies across industries rely on cloud-based human resources systems to hire employees and conduct performance reviews, and to administer benefits and payroll across offices in different countries. The ability to send data across national borders is critical to ensuring companies can coordinate personnel management across a multi-national workforce.

In short, it is difficult to conceive of how commerce in the modern economy could continue to function without the ability to transfer data across international borders. And, in BSA's view, personal data should only be transferred—or used in any way—with real, effective privacy protections. BSA sees no tradeoff between data transfers and data privacy—both are essential. Indeed, BSA has long called for Congress to pass a clear and comprehensive national law that gives consumers meaningful rights over their personal data; imposes obligations on companies to safeguard consumers' data and prevent misuse; and provides strong, consistent enforcement. In all of these conversations, ensuring that companies handle data in privacy-protective ways that honor consumers' expectations is paramount.

Cross border data transfers are critical across all industry sectors. They are also vital to the ability of U.S. companies to grow and compete worldwide. Although most data transfers today involve digital products and services, it would be a mistake to view international data transfers as an issue unique to technology companies. Global companies of all sizes in every industry rely on cross-border data transfers to conduct business, innovate, and compete more effectively. Data transfers are estimated to contribute $2.8 trillion to global GDP—a share that exceeds the global trade in goods and is expected to grow to $11 trillion by 2025.[2] This value is shared by traditional industries like agriculture, logistics, and manufacturing, which realize 75 percent of the value of the Internet.[3] U.S. companies of all sizes and industry sectors must be able to transfer data across borders to complete in a global market.

Indeed, the cross-cutting importance of this issue spurred BSA to launch a new initiative earlier this year—the Global Data Alliance—bringing together companies in industries ranging from consumer goods to healthcare to aerospace technology. Members of the Global Data Alliance provide a diverse range of products and services, serve different types of customers, and operate in different geographic markets—and they all recognize the critical importance of transferring data across borders in a manner that strongly protects personal privacy.

We also should recognize the ultimate beneficiaries of enabling data to travel freely across borders are consumers. Organizations that rely on cross-border data flows

---

[2] OECD, *Measuring the Economic Value of Data and Cross-Border Data Flows,* 297 OECD Digital Economy Papers 24 (Aug. 2020), *https://www.oecd-ilibrary.org/docserver/6345995e-en.pdf?expires=1606762530&id=id&accname=guest&checksum=E07406A96BD78AB99291D0F7D411F923.*

[3] McKinsey Global Institute, *Internet Matters: The Net's Sweeping Impact on Growth, Jobs, and Prosperity* (May 2011), *https://www.mckinsey.com/~/media/McKinsey/Industries/Technology%20Media%20and%20Telecommunications/High%20Tech/Our%20Insights/Internet%20matters/MGI_internet_matters_full_report.ashx.*

produce the food we eat, the cars we drive, the medicines we take, the clothing we wear, and the myriad other goods and services we enjoy. Consumers also depend on these transfers when communicating with loved ones abroad, engaging in banking transactions, and purchasing goods online. The benefits to individuals of online services has been particularly apparent during the COVID–19 pandemic, with studies indicating 50 percent of U.S. employees are working remotely.[4] Moreover, global collaboration between researchers, hospitals, and regulators has been critical to the development and testing of treatments and vaccines for COVID–19.

The importance of cross-border data transfers to the economy will only grow. By 2022, 60 percent of global GDP is expected to be digitized, with growth in every industry driven by data flows and digital technology.[5] By 2025, six billion consumers—amounting to over 75 percent of the world's population—are predicted to be digitally connected, through over 25 billion connected devices.[6] Ensuring data transfers can happen securely and reliably is therefore fundamental not only to current economic growth, but also to future prosperity.

Transatlantic data transfers are particularly important.[7] Data transfers to the EU account for about 50 percent of U.S. data transfers, while data transfers to the United States account for an even greater share of EU data transfers.[8] These data flows are support the roughly $312 billion in annual U.S. services exports to Europe.[9]

These numbers underscore a simple but critically important fact: maintaining stable and secure mechanisms for data transfers between the United States and the European Union is essential to the success of both economies, and to the global economy more broadly.

II. EU-US Data Transfers: The Need for Reliable, Privacy-Protective Mechanisms

The need for specific legal mechanisms to transfer data across the Atlantic is rooted in EU law, and is currently embodied in the EU's General Data Protection Regulation ("GDPR"). Under the GDPR, companies may only transfer personal data from the EU to another country if the country has been deemed to provide an "adequate" level of privacy protection, or if the data is transferred pursuant to a legal mechanism recognized by the GDPR.[10] The European Commission has only recognized twelve countries as providing an "adequate" level of protection. When data is transferred to other countries, then, companies must use another legal mechanism recognized by the GDPR.

The Privacy Shield created a way for companies to transfer data to the U.S. under privacy-protective principles the EU deemed "adequate." By invalidating the Privacy Shield, the *Schrems II* judgment has created an urgent need for a new mechanism for transatlantic data transfers.

Transfer Mechanisms. The GDPR recognizes several legal mechanisms for transferring data across borders, including Standard Contractual Clauses ("SCCs") and Binding Corporate Rules ("BCRs").[11]

- *Standard Contractual Clauses.* SCCs are a standardized set of contractual obligations that companies can adopt when transferring data outside the EU. The SCCs are approved by the European Commission and reflect commitments that implement EU legal requirements to safeguard data. Companies that transfer data pursuant to SCCs typically include the Commission-approved contract language in all of their relevant contracts with suppliers and other vendors. SCCs are widely used, and they underpin transfers of personal data from the EU not

---

[4] Global Data Alliance, *Cross-Border Data Transfers & Remote Work* at 2 (Oct. 5, 2020), *https://www.globaldataalliance.org/downloads/10052020cbdtremotework.pdf.*

[5] Daniel D. Hamilton & Joseph P. Quinlan, *The Transatlantic Economy 2020* at 28 (2020), *https://transatlanticrelations.org/publications/transatlantic-economy-2020/* ("The Transatlantic Economy 2020").

[6] Global Data Alliance, *Cross-Border Data Transfer Facts and Figures, https://globaldataalliance.org/downloads/gdafactsandfigures.pdf* ("GDA Facts and Figures").

[7] Recent studies indicate transatlantic cables carry 55 percent more data than transpacific routes, and the quantity of these transatlantic data transfers are growing rapidly. The Transatlantic Economy 2020 at 41.

[8] BSA | The Software Alliance, *The Future of Transatlantic Data Flows* at 1 (Sept. 23, 2020), *https://www.bsa.org/files/policy-filings/bsa_transatlanticdataflows.pdf* ("BSA Transatlantic Data Flows").

[9] The Transatlantic Economy 2020 at iii.

[10] *See* GDPR, Chapter V. The GDPR took effect in May 2018; the EU's prior data protection law similarly restricted the transfer of personal data to third countries. *See* Directive 95/46/EC.

[11] The other mechanisms include legally binding instruments between public authorities; codes of conduct; and approved certifications. The GDPR also permits companies to transfer data pursuant to derogations for limited, specific situations.

only to the US, but to more than 180 countries. In 2019, one survey found that nearly 90 percent of companies that transferred data outside of the EU relied on SCCs.[12]

- *Binding Corporate Rules.* BCRs are corporate rules that govern international data transfers within a company. The GDPR sets out a list of topics that must be addressed by BCRs, which must specify how the company will apply certain data protection principles and data subject rights to the transferred data. BCRs may take several years to develop and must be approved by a data protection authority in the EU before they can take effect. Even so, their use is limited to a specific set of intra-company transfers; BCRs accordingly do not provide a basis for transferring data to third parties, such as customers, partners, or suppliers.

Privacy Shield. The Privacy Shield provided an important and cost-effective alternative mechanism for transferring data from the EU to the United States. It was negotiated by the U.S. Government and the European Commission to allow companies to commit to privacy principles that ensured data transferred to the U.S. was "adequately" protected. As a result, transfers under the Privacy Shield were deemed "adequate"—thus allowing companies to transfer data from the EU to the U.S. under the Privacy Shield program without using other mechanisms such as SCCs or BCRs.

The Privacy Shield established a voluntary program for companies to transfer data—but once a company publicly committed to comply with its requirements, that commitment becomes enforceable by the Federal Trade Commission. Companies that participate in the Privacy Shield therefore commit to handle data transferred from the EU to the U.S. in line with seven privacy-protective principles on notice, choice, onward transfers, security, data integrity and purpose limitation, access, and enforcement. Participants also adhere to sixteen supplemental principles, which address additional protections for sensitive data and dispute resolution, among other issues. To help ensure these protections remained meaningful in light of changes involving technologies and developments in EU or U.S. law, the Privacy Shield created an internal review mechanism for the United States and the EU to update the Privacy Shield over time. Its most recent annual review, released in October 2019, confirmed that the Privacy Shield remained a trusted mechanism for companies and individuals alike.[13]

The Privacy Shield program was well-used, particularly by small- and medium-sized entities transferring data from the EU. Over 5,300 organizations, in industries ranging from manufacturing to hospitality, participated in the Privacy Shield program,[14] and more than 70 percent of those companies were small- or medium-sized businesses.[15] Its benefits reached more broadly, though, to the networks of suppliers and customers that depended on these Privacy Shield-certified companies.

The U.S. Government also made significant commitments in connection with the Privacy Shield, to address the protection of data transferred under the program. These include not only the annual review mechanism discussed above, but also the establishment of an ombudsperson mechanism, which was designed to respond to requests by EU individuals regarding U.S. signals intelligence practices.[16] Officials at the U.S. Department of Justice and the Office of the Director of National Intelligence also described the many limitations and safeguards applicable to U.S. government access for law enforcement and for national security purposes.[17] These in-

---

[12] IAPP–EY Annual Governance Report 2019 (Nov. 6, 2019), *https://iapp.org/resources/article/iapp-ey-annual-governance-report-2019/* (survey of 370 companies)

[13] European Commission, Report from the Commission to the European Parliament and The Council on the Third Annual Review of the Functioning of the EU-U.S. Privacy Shield, Oct. 23, 2019, *https://ec.europa.eu/info/sites/info/files/report_on_the_third_annual_review_of_the_eu_us_privacy_shield_2019.pdf.*

[14] Congressional Research Service, *U.S.-EU Privacy Shield* (Aug. 6, 2020), *https://fas.org/sgp/crs/row/IF11613.pdf.*

[15] US Department of Commerce Department, Commerce Secretary Wilbur Ross Welcomes Privacy Shield Milestone-Privacy Shield Has Reached 5,000 Active Company Participants (Sept. 11, 2019), *https://www.trade.gov/press-release/commerce-secretary-wilbur-ross-welcomes-privacy-shield-milestone-privacy-shield-has.*

[16] *See* John F. Kerry, Letter to Commissioner Jourova (July 7, 2016), *https://www.privacyshield.gov/servlet/servlet.FileDownload?file=015t00000004q0b.*

[17] *See* Bruce C. Schwartz, Letter to Justin Antonipillai and Ted Dean (Feb. 19, 2016), *https://www.privacyshield.gov/servlet/servlet.FileDownload?file=015t00000004q0W;* Robert Litt, Letter to Justin Antonipillai and Ted Dean (Feb. 22, 2016), *https://www.privacyshield.gov/servlet/servlet.FileDownload?file=015t00000004q1F;* and Robert Litt, Letter to Justin Antonipillai and

Continued

clude Presidential Policy Directive 28 ("PPD–28"), which was issued in 2014 to set out principles and requirements that apply to all U.S. signals intelligence activities. In addition to these commitments, the U.S. Privacy and Civil Liberties Oversight Board has issued oversight reports or conducted oversight reviews of many of these national security authorities.

***Schrems II** Litigation.* The *Schrems II* decision arose after a series of complaints filed by Max Schrems, who in 2013 challenged the predecessor to the Privacy Shield, which was known as the Safe Harbor. In October 2015, the CJEU annulled the Safe Harbor, creating the need for the U.S. and EU to negotiate the Privacy Shield. Later the same year, Schrems filed a reformulated complaint challenging the ability of Facebook to transfer data from the EU to the U.S. using SCCs. Even though the reformulated complaint centered on the use of SCCs, proceedings before both the Irish High Court and the CJEU sparked substantial discussion on the Privacy Shield.

BSA participated in the *Schrems II* litigation as an amicus curiae. We argued before the CJEU, asking it to uphold the SCCs and not address the Privacy Shield, which we felt it did not need to reach in order to decide that case. Throughout the litigation, BSA emphasized SCCs are intended to support transfers to jurisdictions the European Commission has not already deemed "adequate"—and therefore companies using the SCCs should focus on the protections provided by those clauses rather than on the protections offered by the laws of the third country to which data is exported.

In July 2020, the CJEU's *Schrems II* decision invalidated the Privacy Shield, taking away this critical mechanism for transferring data.[18] Importantly, the CJEU did not take issue with the privacy practices of companies that use the Privacy Shield. Rather, the Court based its decision on U.S. intelligence practices it found were not consistent with the EU Charter of Fundamental Rights. The Court focused specifically on signals and intelligence collection under Executive Order 12333 and Section 702 of the FISA Amendments Act of 2008.

At the same time, the CJEU upheld the validity of SCCs. While we agree with the European Commission and the U.S. Government that the safeguards and commitments contained in the Privacy Shield should have been sufficient, we were pleased the Court affirmed the validity of SCCs. Like BCRs, SCCs can create commercial privacy protections beyond those included in the Privacy Shield, because companies may use them to make additional binding commitments.[19] For companies using SCCs, the CJEU stressed the need to determine, on a case-by-case basis and in light of all the circumstances of the transfer, including any additional safeguards that parties may add to SCCs, whether the data can be protected adequately. We agree with that approach. In October, BSA published a set of principles to guide companies in developing additional safeguards for EU–US data transfers. The principles can be turned into specific clauses appropriate to the specific nature of the transfer.[20]

Last month, the European Data Protection Board ("EDPB"), which comprises representatives of the national data protection authorities within the European Union, published draft recommendations for the use of SCCs for transferring data. We understand the concern many companies have raised about whether the recommendations would effectively prohibit transfers to the US. We appreciate that the EDPB has opened its recommendations to public comment. We also respect the difficulty of providing examples that account for all of the circumstances of all data transfers. We remain optimistic the draft recommendations can be revised to better reflect the CJEU's judgment, which envisions greater flexibility and use of additional safeguards to protect privacy. For example, the CJEU's decision directs companies to consider "all" circumstances of a transfer in determining whether additional safeguards are appropriate to supplement SCCs. The full set of relevant circumstances may include the nature of the data transferred and the likelihood of government access to that data, yet the range of these circumstances are not fully reflected in the current draft recommendations.

Despite the widespread use of SCCs, we should not forget that the use of SCCs creates burdens, particularly on smaller businesses that may be forced to re-nego-

---

Ted Dean (June 21, 2016), *https://www.privacyshield.gov/servlet/servlet.FileDownload?file=015t00000004q1A.*

[18] Case C–311/18, *Data Protection Commissioner v. Facebook Ireland Ltd, Maximillian Schrems* (*Schrems II*), ¶¶ 180–85, 191–92, 197–201 (July 16, 2020).

[19] In fact, BSA members were making commitments beyond what is included in Commission-approved SCCs before the *Schrems II* case began.

[20] BSA | The Software Alliance, *Principles: Additional Safeguard for SCC Transfers* (Oct. 2020), *https://www.bsa.org/files/policy-filings/10222020bsasccttransfers.pdf.*

tiate all of their relevant contracts to include terms of SCCs. This option should therefore not be viewed as a replacement for the Privacy Shield. Given the breadth and diversity of companies that rely on transatlantic data transfers, it is imperative to ensure there are multiple practical and privacy-protective ways for companies to transfer data.

III. There is Broad Support for the U.S. Government and the European Commission to Develop an Enhanced Privacy Shield

We commend the U.S. Government and the European Commission for recognizing the need for a new agreement to improve on the Privacy Shield. Shortly after the CJEU's judgment, the Department of Commerce and the European Commission jointly announced the initiation of discussions to evaluate the potential for an enhanced Privacy Shield framework.[21] In doing so, both governments "recognize[d] the vital importance of data protection and the significance of cross-border data transfers to our citizens and economies," and stressed their mutual commitment to supporting privacy, the rule of law, and the close economic relationship between the United States and Europe.[22]

These efforts have strong bipartisan, bicameral support. Again, we very much appreciate the letter Chairman Wicker and Ranking Member Cantwell sent after the *Schrems II* decision to the Commerce Department and the Federal Trade Commission, along with your counterparts on the House Energy and Commerce Committee, encouraging them to work closely with the European Commission to develop a new data transfer mechanism to replace the Privacy Shield.[23]

All sectors of the U.S. economy have also demonstrated support for this effort to reach an improved agreement. BSA and the U.S. Chamber of Commerce led a letter signed by dozens of trade associations spanning a broad range of industries, which together encouraged the U.S. Government to work collaboratively with its EU counterparts to develop a stable and sustainable mechanism to replace the Privacy Shield.[24]

The U.S. Government and the European Commission have also repeatedly expressed their support for the Privacy Shield framework. Prior to the Court's judgment in *Schrems II,* European regulators described the Privacy Shield as a "success story," that offered strong privacy protections to EU data subjects and exemplified the productive partnership between the EU and U.S. governments.[25] In the *Schrems II* litigation, both the U.S. Government and the European Commission argued in support of the Privacy Shield, stressing its importance to both sides of the Atlantic. As an amicus in *Schrems II* and in a separate challenge to the Privacy Shield, BSA argued in support of the Commission and of the Privacy Shield. Moreover, at BSA, we have a longstanding relationship with the European Commission and are committed to working collaboratively and closely with them to address the need for robust data transfer mechanisms and find long-term solutions.

We are confident the U.S. Government and the European Commission can work together to develop an enhanced successor to the Privacy Shield. In its decision invalidating the Privacy Shield, the CJEU focused on concerns around two specific U.S. intelligence-gathering programs, including whether those programs appropriately safeguard privacy and fundamental rights, whether they are subject to independent oversight, and whether they provide EU data subjects with rights to judicial redress. Given the targeted nature of the Court's concerns, we are optimistic the U.S. Government and European Commission can work together to address them. Indeed, it is important to recognize the CJEU expressed no concerns about the adequacy of the privacy protections imposed on commercial entities by the Privacy Shield. Developing an enhanced Privacy Shield should not require a complete overhaul of the existing model but instead should address the specific concerns high-

---

[21] *Joint Press Statement from U.S. Secretary of Commerce Wilbur Ross and European Commissioner for Justice Didier Reynders* (Aug. 10, 2020), *https://www.commerce.gov/news/press-releases/2020/08/joint-press-statement-us-secretary-commerce-wilbur-ross-and-european.*

[22] *Id.*

[23] *Letter from Senator Roger Wicker et al.,* to Secretary Wilbur Ross & Chairman Joseph Simons (Aug. 5, 2020), *https://energycommerce.house.gov/sites/democrats.energycommerce.house.gov/files/documents/FTC.DOC.2020.8.5.%20Letter%20re%20Privacy%20Shield%20ECJ%20Decision.CPC_.pdf.* In addition, several members of the House of Representatives, led by Representatives Welch, LaHood, and DelBene, have echoed this support. *Letter from Representative Peter Welch et al.,* to Secretary Wilbur Ross & Chairman Joseph Simons (Oct. 2, 2020), *https://www.bsa.org/files/policy-filings/10022020congresslettersupportprivacyshield.pdf*

[24] *Letter from BSA* | The Software Alliance *et al.,* to Secretary Wilbur Ross (July 17, 2020), *https://www.bsa.org/files/policy-filings/07172020multiindustryresponselettertoschremsii.pdf.*

[25] European Commission, *EU-U.S. Privacy Shield: Third Review Welcomes Progress While Identifying Steps for Improvement* (Oct. 23, 2019), *https://ec.europa.eu/commission/press corner/detail/en/IP_19_6134.*

lighted in the *Schrems II* judgment. We fully support those efforts and stand ready to provide whatever assistance we can.

IV. Over the Long Term, Countries Must Work Together to Recognize Shared Values on Appropriate Safeguards for Intelligence Practices

The ongoing work by the Administration and the European Commission to develop an enhanced Privacy Shield is urgent, and we appreciate their constructive approach and this Committee's focus on the issue. Creating a new and enhanced mechanism for such transfers is vital to the continued prosperity of both the United States and Europe.

We also urge this Committee, the U.S. Government, and all like-minded democratic societies interested in both security and civil liberties to think boldly about longer-term approaches to security safeguards. Even the CJEU recognizes some amount of signals intelligence is necessary in a democratic society to ensure safety and security. The question is what guardrails and safeguards are needed.

The U.S. Government has, to its credit, publicly released significant guidance about safeguards and oversight mechanisms. It is well positioned to lead a conversation with other governments about the appropriate use of safeguards to protect privacy and fundamental rights, the level of independent oversight, and the ability of individuals to obtain redress for violations. A common understanding on best practices will improve transparency among America's allies and decrease future transatlantic data conflicts.

We have full confidence the U.S. Government and the European Commission can address these issues in the context of developing a successor to the Privacy Shield. At the same time, we recognize commitments and agreements addressing such practices are more durable when they reflect a broader consensus of America and its allies on the appropriate scope of intelligence-gathering practices.

We accordingly encourage the U.S. Government to work with like-minded democratic countries to build a mutual recognition that many countries already share a set of values on the appropriate safeguards for intelligence-collection activities. For example, we support the U.S. Government working toward diplomatic agreements with countries that share our commitment to democracy and the rule of law, to set out a mutual understanding of the types of safeguards appropriate for intelligence-gathering activities to ensure respect for the privacy and fundamental rights of individuals. We do not underestimate the potential magnitude of such an effort, or the challenges it might present. But we believe U.S. leadership on this issue will both strengthen U.S. economic interests, and ensure the United States and its allies can are aligned in promoting economic growth based on the principles of freedom, security, democratic values, and human rights across the globe.

* * *

Thank you again for the opportunity to testify at today's hearing. BSA looks forward to working with the Committee on promoting reliable and secure mechanisms for international data transfers.

The CHAIRMAN. Thank you very much. Since you mentioned the letter, Ms. Espinel, I think we should insert it in the record at this point. So I ask unanimous consent that the letter dated August 5, 2020 to Honorable Wilbur Ross and Honorable Joseph Simons and signed by Frank Pallone Jr., Greg Walden, Roger F. Wicker, and Maria Cantwell be admitted into the record at this point.

[The letter referred to was unavailable at time of printing.]

The CHAIRMAN. Thank you very much. And Mr. Swire, you are next.

STATEMENT OF PETER SWIRE, ELIZABETH AND TOMMY HOLDER CHAIR OF LAW AND ETHICS, SCHELLER COLLEGE OF BUSINESS, GEORGIA INSTITUTE OF TECHNOLOGY

Mr. SWIRE. Chairman Wicker, Ranking Member Cantwell, and members of the Committee for the opportunity to testify today. My name is Peter Swire. I am a Professor at Georgia Tech and Research Director of the Cross-border Data Forum. I have been working on these issues for quite a while. I wrote a book in 1998 for

Brookings on EU-U.S. data privacy fights and have been working on that in some ways ever since. For the *Schrems* trial in Ireland, I submitted testimony of over 300 pages. So I have been living this quite intensively for a long time——

The CHAIRMAN. We won't put that in the record.

[Laughter.]

Mr. SWIRE. There is a nice link in the testimony, sir. This hearing is important in part to create a clear public record about these key issues. The part—one of my testimony makes eight specific points. The first is that the European Data Protection Board has issued draft guidance last month that is so strict it would massively cutoff data flows from the United States—from Europe to the United States. The second point is, a lot of these issues in Europe are constitutional law. And we know from the United States you can't go and amend the Constitution easily.

So the U.S. has to be aware of their Constitutional restrictions as we negotiate eventual solutions. The third point, which has been mentioned by others, is the possibility here of strict data localization if the strict interpretations happen. And at the Cross-Border Data Forum, we are working on additional studies about how serious that would be. Point four is an appendix to my testimony that provides detailed proposals for one of the hard issues here. It is what is called "individual redress," the rules in Europe that there has to be somebody who can check to make sure the citizens' rights are protected.

In August with Kenneth Propp, I wrote a proposal in *Lawfare* on this. There has been comments from a senior European lawyer on it. And in this testimony, I have new non-statutory approaches that presumably could be implemented pretty much immediately that would take big steps toward solving the individual redress problem, and I hope that will be considered quickly. Fifth point has to do with what is called "proportionality" under European law, is there too much surveillance in the view of their judges. There is an Appendix to this testimony that lists all the surveillance updates, it is 25 pages, since 2016. It shows a very strong record in the United States, that safeguards that have been taken since 2016, since the Privacy Shield.

So we have a record to explain to the Europeans the very strong safeguards that exist. A six point and I will take a little bit to expand on this, is that it is important to negotiate a deal, in my view, in the short term, hopefully before January 20. And I would suggest even a one-year deal that would then expire that meets the goals of both the European Union and the United States. For the EU, there have been reports in the press that they would like to have a broader negotiation on many issues, including privacy, with the new Administration.

Having a year to negotiate this as part of a broader deal would meet important European goals. It would also help the European Union on its guidance, clarify things. It would allow additional work on significant U.S. actions, and it would provide time for Congress to see if there are specific statutes that might help. So even a one-year extension would provide a lot of room for what would then lead to presumably a longer term proposal that would build on the shorter term things. That might seem impossible, but hav-

ing this issue negotiated in the first weeks of a new Administration would be very challenging.

So getting something done soon before there is a cutoff of data flows creates a lot more room for better things down the road. In my testimony, the last part about Europe is that as the U.S. considers tough reforms on our side, we should at least understand what they can do on their side. What are their legal options for reform? Those haven't been considered very much in Europe yet, but that is a normal part of negotiations. I then have three points about the U.S. landscape. The first point, which is not fully understood in Europe, is how much continuity we have had on these issues. From the Obama Administration to the Trump Administration on Privacy Shield, on Presidential Directive 28, it has been continuity here, and we would expect the same from a new Biden Administration. So many things are very tough in a partisan world. In this one, there is a lot of agreement.

A second point, which is also been made by others today, is that passing comprehensive commercial privacy legislation would help a great deal. That wouldn't directly address the surveillance issues, but the clear story from Europe is it would help the atmosphere. So if this committee in the Congress could pass a law in that direction, it would make a big difference. It is no small thing. I have worked around this city for a long time, but it would make a huge difference even to have, for instance, a committee bill reported out that showed progress would be a help in the negotiations.

And then the last part of the testimony is why this Congress has a unique opportunity in my 25 years of working on these issues to pass comprehensive privacy legislation. Could I have perhaps 30 or 45 seconds to list a couple?

The CHAIRMAN. Sure.

Mr. SWIRE. OK. And you know better than I all the reasons this is impossible, but not getting there is also a great big problem. So one big reason for hope is the progress that the Chairman and the Ranking Member made in this Congress on a lot of provisions to narrow down the list of disagreements. A second reason is that industry concern about Europe has a strong reason to support legislation.

A third reason that industry after the new California initiative has a strong reason to want to have some restrictions on additional things that are coming in from California. A fourth reason has to do with the favorite issue of preemption, and the testimony suggests one possible way that both sides of that difficult fight could have a victory on preemption, for instance, by allowing the current California privacy law to stay in place, but not having the new initiative go into effect.

There would be some State action, but not other State action that might provide more room. And the last point is, in a Congress where bipartisan accomplishments are difficult, this is an issue where for business and for consumers, for Republicans and Democrats, there may actually be the possibility of bipartisan action.

Thank you, Chairman and Ranking Member, for once again the opportunity for being here today.

[The prepared statement of Mr. Swire follows:]

PREPARED STATEMENT BY PETER SWIRE,[1] ELIZABETH & TOMMY HOLDER CHAIR OF LAW AND ETHICS SCHELLER COLLEGE OF BUSINESS, GEORGIA INSTITUTE OF TECHNOLOGY

Chairman Wicker, Ranking Member Cantwell, and Members of the Committee, thank you for the opportunity to testify today on "The Invalidation of the EU–U.S. Privacy Shield and the Future of Transatlantic Data Flows."

I am Peter Swire, the Elizabeth and Tommy Holder Chair of Law and Ethics at the Scheller College of Business at Georgia Tech, and Research Director of the Cross-Border Data Forum. Since the mid-1990s I have worked intensively on the topic of data flows between the European Union (EU) and U.S., including as lead author of the 1998 *book* called "None Of Your Business: World Data Flows, Electronic Commerce, and the European Privacy Directive." I have worked on these issues as a government official and private citizen, and wrote *expert testimony* of over 300 pages for the 2017 trial in Ireland of the *Schrems II* case. A biography appears at the end of this testimony.

This hearing is important in part to create a clear public record about these complex and important issues concerning the European Union, the United States, and international flows of "personal data," which is often called PII or "personally identifiable information" in the U.S.

Part I of this testimony offers observations on legal and policy issues in the European Union. Key points include:

A. The *European Data Protection Board* in November issued draft guidance with an extremely strict interpretation of how to implement the *Schrems II* case.

B. The decision in *Schrems II* is based on *EU constitutional law.* There are varying current interpretations in Europe of what is required by *Schrems II,* but constitutional requirements may restrict the range of options available to EU and U.S. policymakers.

C. Strict EU rules about data transfers, such as the draft EDPB guidance, would appear to result in *strict data localization,* creating numerous major issues for EU-and U.S.-based businesses, as well as affecting many online activities of EU individuals.

D. *Appendix 1* to this testimony provides detailed proposals for one of the requirements of the EU Charter—*individual redress* for violation of rights in the U.S. surveillance system.

E. Along with concerns about lack of individual redress, the CJEU found that the EU Commission had not established that U.S. surveillance was "proportionate" in its scope and operation. *Appendix 2* to this testimony seeks to contribute to an informed judgment on *proportionality,* by cataloguing *developments in U.S. surveillance safeguards since* the Commission's issuance of its *Privacy Shield decision in 2016.*

F. Negotiating an EU/U.S. adequacy agreement is important in the *short term.*

G. A short-run agreement would assist in creating a better overall *long-run* agreement or agreements.

H. As the U.S. considers its own possible legal reforms in the aftermath of *Schrems II,* it is prudent and a normal part of negotiations to seek to understand *where the other party—the EU—may have flexibility to reform its own laws.*

Part II of the testimony provides observations on the U.S. political and policy landscape:

A. Issues related to *Schrems II* have largely been bipartisan in the U.S., with *substantial continuity* across the Obama and Trump administrations, and expected as well for a Biden administration.

B. *Passing comprehensive privacy legislation would help* considerably in EU/U.S. negotiations.

C. This Congress may have a *unique opportunity to enact comprehensive commercial privacy legislation* for the United States.

---

[1] Elizabeth and Tommy Holder Chair of Law and Ethics, Georgia Tech Scheller College of Business; Research Director, Cross-Border Data Forum; senior counsel, Alston & Bird LLP. The opinions expressed here are my own, and should not be attributed to the Cross-Border Data Forum or any client.

PART I: Observations on Legal and Policy Issues in the European Union

In the wake of the *Schrems II* decision very large data flows from the EU to the U.S. and other third countries may become unlawful. The likelihood and magnitude of such a blockage are uncertain, and depend significantly on how European actors interpret the *Schrems II* decision. With Kenneth Propp, I have written *previously* on the background of the *Schrems II* case, its holdings, and its geopolitical implications. In Part I of this testimony, I address legal and policy issues specifically about the EU.

A. The European Data Protection Board in November issued draft guidance with an extremely strict interpretation of how to implement the ***Schrems II*** *case.*

An apparently very strict interpretation of *Schrems II* appears in two documents issued, subject to public comment, by the European Data Protection Board on November 11, 2020. My discussion here draws on the clear and expert three-part commentary of Professor Théodore Christakis in the *European Law Blog.* As the body of national data protection regulators, the EDPB's views are important due to its official role in interpreting the GDPR as well as language in the *Schrems II* decision about its role in defining what supplementary safeguards are sufficient for transfers outside of the EU.

The EDPB issued its draft of the "*European Essential Guarantees for Surveillance Measures*" ("EEG Requirements"). This document summarized the fundamental rights jurisprudence of the European Court of Human Rights (housed in Strasbourg, and interpreting the European Convention on Human Rights) and the Court of Justice of the European Union (housed in Luxembourg, and interpreting European Union law including the EU Charter of Fundamental Rights). A key task of the EEG Requirements was to state the EDPB's understanding of what legal requirements a third country must have in order to "offer a level of protection essentially equivalent to that guaranteed within the EU." To simplify the EDPB's main point—if a third country (such as the U.S.) meets the EEG Requirements, then the country can be seen as providing "essentially equivalent" protections; if not, then the country does not provide "essentially equivalent" protections, and transfers of personal data would require additional safeguards.

Where "essentially equivalent" protections exist, then transfers to that country may be found "adequate" under EU law. This sort of "adequacy" determination was made by the EU Commission in 2016 for the Privacy Shield. Eleven countries currently have this sort of adequacy determination by the EU Commission. A new EU/U.S. agreement would presumably be based on a similar adequacy finding.

If an adequacy determination is not in place, then the *Schrems II* court stated that transfers from the EU to a third country can exist where "supplementary measures" or "additional safeguards" are in place. Along with the EEG Requirements, the EDPB released its "*Recommendations on Supplementary Measures*" on November 11. Prior to the EDPB guidance, the U.S. government issued its "*White Paper*" on "Information on U.S. Privacy Safeguards Relevant to SCCs and Other EU Legal Bases for EU–U.S. Data Transfers after *Schrems II.*" Other expert commentators published detailed *studies* of how additional safeguards, well implemented, could create a lawful basis for continuing to use Standard Contractual Clauses or other mechanisms for transferring personal data from the EU to third countries including the U.S.

As Professor Christakis has explained, the EDPB interpreted the *Schrems II* decision to be far stricter than had the White Paper or other commentators. *The EDPB's EEG Requirements are so strict, as Christakis* ***wrote****, that "third countries might rarely if ever meet the EEG requirements." Data exporters, under the EDPB approach, would then have to rely on its Recommendations on Supplementary Measures. Christakis, however,* ***found*** *these are also exceptionally strict: "To sum up, the EDPB's guidance clearly indicates that no data transfer should take place to non-adequate/non-essentially equivalent countries unless the data is so thoroughly encrypted or pseudonymised that it cannot be read by anyone in the recipient country, not even the intended recipient."*

B. The decision in ***Schrems II*** *is based on EU constitutional law. There are varying current interpretations in Europe of what is required by* ***Schrems II,*** *but constitutional requirements may restrict the range of options available to EU and U.S. policymakers.*

There are important and as-yet unresolved disagreements among EU experts about how to interpret the *Schrems II* decision. Disagreements about constitutional law are certainly familiar to the Senators and American lawyers. That sort of disagreement is what exists in Europe in the aftermath of *Schrems II.*

Much of the *Schrems II* decision relied on specific provisions in the *EU Charter of Fundamental Rights,* which came into force in 2009 along with the Treaty of Lisbon:

1. Article 47 of the Charter addresses the right to an effective remedy: "Everyone whose rights and freedoms guaranteed by the law of the Union are violated has the right to an effective remedy before a tribunal." Appendix 1 to this testimony examines issues arising under Article 47, notably what sorts of individual redress the U.S. might provide for EU persons with respect to U.S. surveillance practices.
2. Article 7 of the Charter addresses respect for privacy and family life: "Everyone has the right to respect for his or her private and family life, home and communications." This right to privacy is similar to the "right to respect for private and family life" in Article 8 of the *European Convention of Human Rights,* first signed in 1950.
3. Article 8 of the Charter is a data protection right. It states: "(1) Everyone has the right to the protection of personal data concerning him or her; (2) Such data must be processed fairly for specified purposes and on the basis of the consent of the person concerned or some other legitimate basis laid down by law. Everyone has the right of access to data which has been collected concerning him or her, and the right to have it rectified. (3) Compliance with these rules shall be subject to control by an independent authority."

The EDPB guidance can illustrate the importance of how these fundamental rights protections will be interpreted after the *Schrems II* decision. To illustrate, suppose that each aspect of the draft EDPB guidance were required by the Charter of Fundamental Rights. In that instance, the European Union would have no legal authority to weaken constitutional protections, and the strict prohibitions on data transfers under the EDPB draft guidance would be required as a matter of EU constitutional law. Based on the review of that guidance by Professor Christakis, an enormous range of flows of personal data would be prohibited to the U.S., China, India and most or all other third countries in the world (except the small number with a current adequacy decision in place).

The draft EDPB guidance, in fact, would appear to be clearly stricter than constitutionally required by the *Schrems II* decision. After all, the CJEU went to considerable lengths to say that transfers using Standard Contractual Clauses remained lawful where "additional safeguards" were in place; however, the EDPB guidance found no "additional safeguards" that would enable access to the personal data in a third country. It appears that the EDPB draft guidance would render the CJEU's discussion of additional safeguards to be a nullity.

Based on my discussions with other EU legal experts, many EU legal experts would find greater flexibility under EU constitutional law than provided by the EDPB draft guidance. Going forward, EU experts on fundamental rights will engage on what restrictions on data transfers are required by the Charter of Fundamental Rights, as contrasted with decisions of non-judicial officials.

In conclusion on EU constitutional requirements, a very strict interpretation of the decision may leave limited options open for policymakers. Going forward, EU experts on fundamental rights will engage on what restrictions on data transfers are required by the Charter of Fundamental Rights, as contrasted with decisions of non-judicial officials. Although the precise legal issues are different, the importance of constitutional doctrine is well known to U.S. lawmakers for free speech and other First Amendment issues. *Members of this Committee will therefore understand that legal, constitutional limits may affect what the EU Commission, the European Parliament, and other EU institutions can do in the wake of the* ***Schrems II decision.***

C. Strict EU rules about data transfers, such as the draft EDPB guidance, would appear to result in strict data localization, creating numerous major issues for EU-and U.S.-based businesses, as well as affecting many online activities of EU individuals.

The European Union will continue its own deliberations about how strict are the limits on data flows, as a matter of either EU policy choices or fundamental rights jurisprudence. I will briefly discuss some practical effects of a strict approach, which appear considerable.

I will first address what one might call the "boy who cried wolf" theory. After all, concerns about EU cut-off of data have arisen repeatedly since the Data Protection Directive went into effect in 1998. At that time, the EU/U.S. Safe Harbor, and other practical measures, enabled commerce to proceed without great hindrance. Later, in 2015, the CJEU issued the first *Schrems* decision, and privacy experts advised companies that data flows from the EU might be cut. Then, the EU and U.S. negotiated

the Privacy Shield, and commerce continued. More recently, the General Data Protection Regulation (GDPR) went into effect in 2018, along with warnings that it could shut down numerous business models. In practice, after often-considerable compliance efforts, most business has been able to continue under GDPR. After these three rounds of warnings of disaster that didn't materialize, it would be easy for people to assume that the aftermath of *Schrems II* will once again be less impactful on data transfers than doomsayers cry out.

My view, however, is that the possibility of major disruptions of data flows is far greater this time. The CJEU—the supreme court of Europe, whose decisions are binding on the member states—has reiterated its strong concerns about transferring data to countries whose surveillance systems fail to meet European standards. That same court would have the final word about any new EU–U.S. agreement, or any other legal mechanism that seeks to enable transfers to third countries. Depending on how one interprets the constitutional dimensions of *Schrems II* and the many other high court decisions examined by the EDPB, the apparent room for policymaker discretion now seems more limited. In addition, based on my discussions with knowledgeable persons, there is a significant possibility that one or more of the largest companies in the world may come under court order to stop transfers, before the January 20 U.S. presidential inauguration. In short, this time may fit the old story, where the boy cried wolf once again, but this time the wolf was really there.

If many data transfers are cut off, then the effect would be data localization. The term "local" here would apply to the EU member states, the other countries in the European Economic Area, and the currently eleven countries that now have an adequacy determination. Transfers to the United Kingdom after the January 1, 2021 Brexit would appear to depend on the UK receiving an adequacy determination, which is currently being considered but has not been finalized.

As the possibility of data localization increases, it becomes increasingly important for organizations to determine what it would mean to implement localization, and for policymakers to understand the effects of localization. The most detailed examination of such data flows, of which I am aware, remains the book that I wrote with Robert Litan in 1998, called "None of Your Business: World Data Flows, Electronic Commerce, and the European Privacy Directive." Thanks to permission from its publisher, the Brookings Institution, that book is now downloadable from the Brookings *website.* Chapter 5 of the book addresses "privacy issues affecting many organizations," such as human resources, auditing, business consulting, and customer support such as call centers. Chapter 6 examines financial services in detail, and the effects on that large sector deserve careful attention. Chapter 7 looks at "other sectors with large trans-border flows", including business and leisure travel and e-commerce generally; it also looks at possible interruptions of pharmaceuticals research, which would be especially important to consider during the COVID pandemic, when sharing of personal data might be so important concerning the safety and efficacy of vaccines as well as other medical information.

Looking ahead, I plan to work with the Cross-Border Data Forum as soon as possible to update and extend the data localization analysis. I hope to publish initial pieces of that analysis in time to offer comments on the EDPB Guidelines, due December 21. Many types of data flows are the same as in 1998, but there are important new categories of data flows, perhaps most notably for cloud computing, where the personal data of individuals is often stored in a different country. Several current reports are also available that provide useful discussion of the impacts of cutting off data, including *here* and *here.* I welcome any information or suggestions about how to accurately describe the effects of data localization, such as under a strict interpretation of EU law.

Pending such additional study, I offer the following observations about the effects of a strict requirement of data localization:

1. *Companies may find it difficult or impossible to "fix" the problem themselves*—the legal problem concerns the rules for government access to personal data.
2. *Data localization would have enormous impacts on third countries other than the U.S. Schrems II* clarified that its rule apply to the U.S. in particular but also to all third countries that lack essentially equivalent protections.
    a. Some countries, such as China, have woefully *weaker safeguards* against government surveillance than the U.S. does. It is therefore difficult for me to understand what additional safeguards might be taken to enable transfers to such countries. China is Germany's largest trading partner, illustrating the large effect on the EU (rather than the U.S.) of strict limits on transfers.
    b. Other countries, such as Canada, are democracies with strong privacy regimes, but have not thus far received an adequacy determination. Even if

the EU and U.S. reach an agreement, there will be legal uncertainty about whether and how transfers can continue to these other democracies.

3. Particular study should focus on the *effects on EU individuals,* who may lose access to services and face reduced choice about how to live their online life. Similarly, *EU-based businesses* may face serious obstacles, beginning but not limited to how they operate with their non-EU affiliates, suppliers, and partners. Detailed study of the effect on the EU will help EU decisionmakers weigh how to protect privacy while also meeting other goals, as stated by the CJEU in *Schrems II,* that are "necessary in a democratic society."
4. During *the coronavirus pandemic,* individuals and businesses rely more than ever before on online services, many of which are operated or managed across borders. Disruptions from data localization thus would appear to be especially great until we reach a post-pandemic time.
5. In conclusion on the effects of a strict EU approach, it is vital to consider carefully what measures can satisfy all the relevant legal constraints. New solutions quite possibly are necessary to enable continued data flows along with the legally-required improvements in privacy protection.

D. Appendix 1 to this testimony provides detailed proposals for one of the requirements of the EU Charter—individual redress for violation of rights in the U.S. surveillance system.

This testimony will briefly summarize key points from Appendix 1, which provides details on how the U.S. might craft a new system of individual redress to address the CJEU's concerns. The Appendix has three parts:

1. Discussion of the *August 13 proposal* by Kenneth Propp and myself, entitled *"After Schrems II: A Proposal to Meet the Individual Redress Problem."* In order to provide an effective fact-finding phase, a statute could create a mandate for intelligence agencies to conduct an effective investigation when an individual (or a Data Protection Authority on behalf of the individual) makes a complaint. This mandate is similar to the Freedom of Information Act—an individual does not have to show specific injury in order to make a FOIA request, and an individual similarly would not need to show injury to request the investigation. Once the fact-finding is concluded, the statute could provide for appeal to the Foreign Intelligence Surveillance Court (FISC).
2. Discussion of the article by *European legal expert Christopher Docksey* on *"Schrems II and Individual Redress—Where There's a Will, There's a Way."* This article found the Propp/Swire approach promising, while pointing out important aspects of EU law to be considered in any U.S. system for individual redress.
3. *New material about how the individual redress system could be created, even without a new statute.* In the fact-finding phase, Executive Branch agencies could be required to perform an investigation pursuant to a new Executive Order or other presidential action. An independent agency, such as the Privacy and Civil Liberties Oversight Board, could sign a memorandum of understanding that would bind the agency to participate in the process. One the fact-finding is complete, complaints that concern surveillance under Section 702 FISA could then go to the FISC. The FISC has continuing oversight of actions pursuant to its annual court order concerning Section 702. It appears that the government could promise to report the outcome of an investigation to the FISC, and the FISC could then review the fact-finding investigation to determine whether it complied with its court order.

As discussed in Appendix 1, "non-statutory approaches are worth considering even if a somewhat better system might be created by a statute. A non-statutory approach quite possibly is the best way to ensure that data flows and privacy protections exist during an interim period while legislation is being considered."

Based on my experience, the fundamental rights orientation of EU data protection law has often emphasized the importance of a mechanism for an individual to make a complaint or access request. Then, there must be a mechanism with sufficient independence and authority to review the facts and issue an order to correct any violations. As the CJEU re-emphasized in *Schrems II,* Article 47 of the Charter requires "an effective remedy before a tribunal." *After working extensively on this subject, and speaking with both European and American experts, I believe it is vital and apparently feasible to construct a new system of individual redress with respect to actions by U.S. surveillance agencies. Creating such a system would directly respond to a repeated and important criticism to date of the "essential equivalence" of U.S. protections.*

E. Along with concerns about lack of individual redress, the CJEU found that the EU Commission had not established that U.S. surveillance was "proportionate" in its scope and operation. Appendix 2 to this testimony seeks to contribute to an informed judgment on proportionality, by cataloguing developments in U.S. surveillance safeguards since the Commission's issuance of its Privacy Shield decision in 2016.

Along with lack of individual redress, the *Schrems II* court found that the principle of proportionality requires that a legal basis which permits interference with fundamental rights must "itself define the scope of the limitation on the exercise of the right concerned and lay down clear and precise rules governing the scope and application of the measure in question and imposing minimum safeguards." (¶ 180). The court held that the 2016 Privacy Shield adequacy decision by the EU Commission did not show proportionality for Section 702 and EO 12,333. (¶ 184).

Concerning the issue of proportionality, I offer six observations:

1. Appendix 2 to this testimony provides "Updates to U.S. Foreign Intelligence Law since 2016 Testimony." Appendix 2 presents updates on the U.S. legal and regulatory regime for foreign intelligence surveillance that have occurred since *testimony* of over 300 pages that I provided to the Irish High Court in 2016 on the same subject (the "2016 Testimony"). *Taken together, the 2016 Testimony and Appendix 2 seek to present an integrated set of references that may inform ongoing assessments,* under European Union law, *of the proportionality and overall adequacy of protection* of personal data related to U.S. foreign intelligence law.
2. A proportionality assessment is quite different than the issue of individual redress. Redress is a specific assessment—a sufficient redress provision exists or it doesn't. by contrast, *"proportionality" can be a more wide-ranging and fact-based assessment, similar to defining a term such as "reasonable."*
3. As a related point, the *Schrems II* decision cites European law that privacy and data protection rights "are not absolute rights," but instead "must be considered in relation to their function in society. (¶ 172) In addition, standard data protection clauses are lawful "where do not go beyond what is necessary in a democratic society to safeguard, inter alia, national security, defence and public security." (¶ 144). *More documentation may thus be relevant as evidence of what is "necessary in a democratic society."*
4. Appendix 1, concerning individual redress, discusses the possibility of incorporating concepts such as *proportionality* and necessity, or related terms used in U.S. law, into the *targeting procedures for Section 702* approved annually by the FISC. I make this proposal for the first time in this testimony, and so there may be classified or other persuasive reasons why such an approach is inadvisable or unlawful.
5. In considering whether and how to issue an updated adequacy opinion about the United States, the EU Commission will thus have available *a considerable record that evidences the large number and high quality of safeguards within the U.S. surveillance system.* Chapter 6 of my 2016 Testimony cited a *study* led by Ian Brown, then of Oxford University, that concluded that the U.S. legal system of foreign intelligence law contains "much clearer rules on the authorization and limits on the collection, use, sharing, and oversight of data relating to foreign nationals than the equivalent laws of almost all EU Member States." The U.S. government's White Paper this fall adds particulars about current safeguards.
6. With that said, European law to date has indicated that *"essential equivalence" of a third country is judged against the standards set forth by the CJEU, rather than a comparison of U.S. practices to the practices of the EU member states.* Professor Kristina Irion this year has *explained* the relevant EU doctrine. Supporters of U.S. or other third country adequacy might therefore complain about hypocrisy or an unfair standard, but such arguments to date have not prevailed in European courts.

In conclusion on proportionality, it is important for the United States and the EU Commission to develop a strong record for why Section 702 and other surveillance programs currently are "proportionate," or else consider reforms that do establish proportionality.

F. Negotiating an EU/U.S. adequacy agreement is important in the short term.

There are strong reasons for the EU and the U.S. to seek agreement in the short term, so that the EU Commission can issue an adequacy decision. I highlight five points:

1. *Especially in the wake of the very strict EDPB draft guidance, there is now considerable uncertainty about the lawful basis for many transfers from the EU to third countries, including the U.S.* As mentioned above, there may well be court orders issued, even before January 20, that prohibit transfers of personal data by one or more major companies based in the U.S.
2. My understanding is that the current administration has a process in place to engage immediately with the EU. Even though a Biden administration would have available experts on these EU/U.S. data issues, *there could be a disruptive delay after January 20 if discussions are not completed by then. The immediate discussions should take account of the legal and political realities facing the EU Commission*—it will only wish to enter into an agreement with a strong case that it is acting consistent with the CJEU decision in *Schrems II*. The U.S. thus has a stronger-than-usual incentive to make its "best and final offer" quickly, because of the limited time to renegotiate before January 20.
3. *To avoid potentially large disruptions, it makes sense to achieve a short-term package even if additional reforms and agreements may be possible in the longer-run.* For instance, an adequacy decision might be for a limited time, such as one year. That would provide a new administration and the EU time to develop longer-term agreements across both data protection and other issue areas, as the EU has *indicated* it would like to do. A deadline, such as one year, would provide a useful incentive for all concerned to continue to work intensively toward a longer-term solution.
4. *Any short-term approach should include, if possible, clear attention to key sectors, including medical research and financial services.* During the pandemic, it would be foolhardy to interrupt the ability of medical researchers and manufacturers to develop and test for the safety and efficacy of COVID–19 treatments and vaccines. In addition, the financial services sector has historically relied primarily on Standard Contractual Clauses for transfers, rather than Privacy Shield. My understanding is that to date there has been low risk within the EU of enforcement against the financial services sector, which I believe transfers large amounts of personal data daily for business and regulatory reasons. With strict approaches such as the EDPB draft guidance, there is now increased risk of disruption of the global financial system due to possible limits on transfers of personal data from the EU to third countries.
5. *There is an important reason, from the EU perspective, to issue an adequacy decision for the U.S. in the short term, even though* ***Schrems II applies to third countries generally.*** The specific judicial findings in Europe have been about essential equivalence and the U.S., even though the U.S. has stronger safeguards than most or all other countries for foreign intelligence surveillance and privacy. *An adequacy decision initially concerning the U.S. thus provides the EU time to clarify its overall approach for transfers to third countries.* Enforcement actions can meanwhile proceed with respect to other third countries, such as China, to enable the EU judicial process to make findings relevant to multiple third countries, and avoid a discriminatory impact on an allied nation—the U.S.—that has many safeguards already in place.

G. A short-run agreement would assist in creating a better overall long-run agreement or agreements.

As discussed through this testimony, there are urgent short-term difficulties concerning the lawful basis for transfers of personal data from the EU to third countries. I next explain four reasons why an adequacy agreement in the near future would assist in creating a better overall set of reforms and agreements in the longer-run:

1. In this testimony, I am suggesting the desirability of seeking an adequacy agreement in the short run, such as for one year. *This sort of breathing period would enable a new administration to engage systematically to create durable approaches for agreements with the EU on data protection and other issues.*
2. A short-term agreement would *provide the Congress with time to consider any legislation that may assist in creating a durable approach* to enabling trans-Atlantic transfers while also protecting privacy, meeting EU and U.S. legal requirements, and achieving other goals including national security. As one example, non-statutory approaches for individual redress may be possible, as explained in Appendix 1, but a subsequent statute might improve on the non-statutory approach.
3. One category of legislation to consider is for *the U.S. to codify in statute safeguards that already exist in practice.* One example would be the protections for

the personal data of non-U.S. persons, as provided currently in PPD–28. More broadly, Appendix 2 to this testimony provides examples of privacy-protective practices that currently exist but are not explicitly set forth by statute. This sort of codification could address EU concerns that informal guidance or even agency policies are not "established in law" as effectively as a statute or other binding legal instrument.

4. *On an even longer time scale, there are strong reasons for the U.S., the EU, and democratic allies to engage systematically on a realistic and protective set of guidelines for government access to personal data held by the private sector.* Such a process should include input from a range of expert stakeholders, including data protection/privacy experts but also experts in areas such as national security, law enforcement, and economic policy. I understand the OECD may move forward with such an initiative, first proposed by Japan, on "free flow of data with trust" with respect to government access to data held by the private sector. Such guidelines, among other goals, could help define what safeguards are "necessary in a democratic society," both to protect fundamental rights and achieve other compelling goals.

H. As the U.S. considers its own possible legal reforms in the aftermath of ***Schrems II,*** *it is prudent and a normal part of negotiations to seek to understand where the other party—the EU—may have flexibility to reform its own laws.*

For understandable reasons, the bulk of discussion to date has focused on what reforms the U.S. might consider in order to meet legal requirements set forth in *Schrems II* and other CJEU decisions. With that said, my testimony today discusses reasons to seek both short-term and longer-term agreements with the EU on cross-border data issues. It is normal and prudent, in any negotiation, to understand where each party may have flexibility to negotiate. As one example, my view is that the U.S. should seriously consider reforms to enable individual redress for EU citizens related to U.S. surveillance activities. Where might the EU also consider reforming any aspect of its regime?

Recognizing that views might vary about what is possible as a legal or policy matter, I offer four observations:

1. For reasons discussed above, I believe there is room, consistent with the *Schrems II* decision, for the EDPB to make changes to its draft guidance—the CJEU contemplated some continuation of transfers where additional safeguards are in place, but the draft guidance is so strict that such transfers in practice appear to be eliminated. The analysis by *Professor Théodore Christakis examines specific ways the EDPB guidance might be amended consistent with EU law.*
2. Chapter V of the GDPR governs "transfers of personal data to third countries or international organizations." Article 46 of GDPR sets forth extensive measures to enable lawful transfers to third countries that have not received an adequacy determination under Article 45. A similar approach existed under Article 26 of the Data Protection Directive, which applied from 1998 until GDPR went into effect in 2018. If the EU came to the view that Article 46 had been interpreted more narrowly than intended, then *the EU could at least contemplate a targeted amendment to GDPR to clarify its intent to allow transfers under Article 46 with defined, appropriate safeguards.* Any such amendment might be politically painful and challenging within the EU; massive disruptions of global trade would also be painful and challenging.
3. *The legal basis for transfers to the U.S. might be stronger if the U.S. and the EU negotiated a formal international agreement, such as a treaty.* I have seen draft scholarship, not yet public, that indicates that the legal basis for transfers from the EU to a third country such as the U.S. might be stronger if done pursuant to a formal international agreement, such as a treaty. The Safe Harbor and Privacy Shield were not treaties. Such a treaty would presumably not be negotiated or implemented in the short term, but may be a useful longer-term approach.
4. *By contrast, in discussions with EU experts, they have clearly stated that an amendment to the Charter of Fundamental Rights would be extremely difficult or impossible to consider.* Americans can readily understand this view—imagine if another country insisted that the U.S. amend the First Amendment free speech guarantees. It will thus be important, as a matter of EU law, to understand what is required under the Charter. The Commission, Parliament, and other EU institutions are legally bound to follow the Charter, but have room outside those requirements to make decisions within their competence.

To date, there has been little or no visible discussion within the EU about reforming its own data protection laws, such as considering any change to GDPR. In discussing possible changes, I am not seeking to tell the EU how to write its own laws. *The limited point here is that the U.S. and other third countries, in contemplating difficult reforms to their own laws, can reasonably at least consider how the EU might make reforms as well. Any eventual agreements can then be built on an understanding of what is or is not legally possible within each legal system.*

PART II: Observations on U.S. Political and Policy Landscape

A. Issues related to ***Schrems II*** *have largely been bipartisan in the U.S., with substantial continuity across the Obama and Trump administrations, and expected as well for a Biden administration.* Issues related to the Privacy Shield, *Schrems II,* and trans-Atlantic data flows have been far more bipartisan in the U.S. than for many other policy issues. I briefly highlight six aspects of continuity

1. *Privacy Shield.* The EU–U.S. Privacy Shield was signed in 2016, under President Obama. The Trump administration has uniformly supported the Privacy Shield, including working closely with EU officials in its annual reviews.
2. *Enforcement by the Federal Trade Commission.* The FTC is an independent agency, charged with enforcing violations of the Privacy Shield, as part of its general authority to protect privacy and enforce against unfair and deceptive acts. Change in administration, in my view, has not affected and will not affect the FTC's commitment to enforce company commitments to protect privacy in cross-border data flows.
3. *PPD–28.* President Obama issued PPD–28, with its safeguards for non-U.S. persons in signals intelligence, in 2014. PPD–28 has remained in force under President Trump.
4. *Surveillance transparency and safeguards generally.* Appendix 2 to this testimony reports on safeguards and other developments in surveillance since the Privacy Shield was negotiated in 2016 and I provided my expert testimony in Ireland. The consistent theme in Appendix 2 is how transparency and surveillance safeguards have continued extremely similarly under the Obama and Trump administrations.
5. *Continued attention both to privacy and other goals such as national security.* As a member in 2013 of the *Review Group* on Intelligence and Communications Technology, I observed how seriously U.S. government officials treated both privacy and other important goals such as national security. My opinion is that similar attention to these goals has continued and will continue for each U.S. administration.
6. *A Biden administration can draw upon experts in these EU/U.S. data issues.* Another reason to expect policy continuity is that the Biden administration will have available experts in Privacy Shield and other EU/U.S. data issues. For example, key negotiators of the Privacy Shield, as signed in 2016, were Ted Dean, then in the U.S. Department of Commerce, and Robert Litt, then General Counsel for the Office of the Director of National Intelligence. Both Mr. Dean and Mr. Litt have been named as members of the Biden-Harris transition team.

In short, even though there are many differences on other policy matters, what is remarkable for EU/U.S. data issues is bipartisan agreement on issues of trans-Atlantic data flows.

B. Passing comprehensive privacy legislation would help considerably in EU/U.S. negotiations.

I believe that enactment of comprehensive commercial privacy legislation would greatly improve the overall atmosphere in Europe for negotiations between the EU and the U.S. about the effects of *Schrems II.*

This conclusion may seem counter-intuitive. After all, the CJEU holdings concerned only issues of U.S. intelligence access to personal data. By contrast, a commercial privacy statute would apply exclusively or primarily to private-sector processing of personal data. As a strict legal matter, a comprehensive commercial privacy law in the U.S. would not address the holdings in *Schrems II.*

Nonetheless, I am confident that a meaningful, protective commercial privacy bill would make an important difference. That is not only my own intuition, developed after a quarter-century of working on EU/U.S. data issues. In addition, I have asked the question to multiple European experts. *Their response has been unanimous and positive, along the lines of "Yes, that would make a big difference."*

Here are a few reasons to think enacting a comprehensive commercial privacy law would help:

1. *We have seen the link previously between U.S. intelligence surveillance and the EU reaction on commercial privacy.* The clearest example is what happened after the Snowden revelations began in June, 2013. Before that, it looked like the draft of GDPR was blocked or moving slowly through the EU Parliament. After that, GDPR was amended in multiple ways to be considerably stricter, including on the U.S.-led tech sector. GDPR passed the Parliament overwhelmingly in early 2014 by a 621–10 margin. EU Vice President Viviane Reding, in her official statement on the vote, specifically referenced *"the U.S. data spying scandals"* as a reason for passage.
2. *The U.S. may soon become the only major nation globally that lacks a comprehensive commercial privacy law.* Whatever a person's views may be of the best approach to protecting privacy, the global trend is unmistakably in one direction—toward each country having a comprehensive commercial privacy law. Professor Graham Greenleaf in Australia has carefully *documented* these trends: "The decade 2010–2019 has seen 62 new countries enacting data privacy laws, more than in any previous decade, giving a total of 142 countries with such laws by the end of 2019." Perhaps more importantly, the four most significant recent exceptions to such a law have been the U.S., Brazil, India, and China. Brazil's new privacy law went into effect in 2020. India has nearly finished its parliamentary process to pass its law. China is also moving forward with a commercial privacy law (although its protections against government surveillance remain *far weaker* than in the U.S.). Simply put, unless the U.S. acts in the next Congress, the U.S. may be the only major nation globally that lacks a comprehensive privacy law.
3. A U.S. privacy law would strengthen the hand of U.S. allies in the EU. Currently, there are many in Brussels and throughout the EU who favor retaining a strong alliance generally with the U.S. That support for remaining allies was reflected, for instance, in the broad EU Commission draft, reported by the *Financial Times,* that "seeks a fresh alliance with U.S. in face of China challenge." More specifically, as seen for instance in a recent DigitalEurope *study* on the effects of *Schrems II,* many in Europe understand the harsh consequences to Europeans themselves of a major cut-off in data flows.

   From the European perspective, the 2000 Safe Harbor agreement and the 2016 Privacy Shield are examples of "special deals" that make transfers to the U.S. easier than transfers to the other countries in the world that lack a general adequacy finding. As the U.S. becomes an increasingly glaring exception on privacy laws, it becomes more and more difficult for those in Europe to explain why the U.S. should be a favored partner. *Put bluntly, the U.S. as the last holdout on a privacy law can look more like a "privacy pariah" than a "favored partner."* By contrast, enacting a U.S. commercial privacy law sends the message that the U.S. in general offers legal protections for privacy. With a U.S. privacy law in place, it becomes far easier in Brussels and the EU generally to complete a privacy deal with the U.S. As a related point, *serious progress on U.S. privacy legislation during the next two years, such as passage in a crucial committee such as Senate Commerce, can itself help foster progress in EU/U.S. negotiations by showing that passage of a U.S. privacy law is feasible.*

C. This Congress may have a unique opportunity to enact comprehensive commercial privacy legislation for the United States.

You as Senators have far greater insight than an outside observer can have about what is possible to enact in this Committee, the Senate, or the Congress in the next two years. With that said, *my own perspective is that the 117th Congress, convening this January, has the best chance to enact comprehensive Federal privacy legislation that I have ever seen.*

I offer six reasons for believing that now is an unusual opportunity to pass privacy legislation:

1. *This Committee has already made a great deal of progress on finding areas of agreement between the political parties.* In 2020, there was significant convergence on draft legislation supported, separately, by Chairman Wicker and Ranking Member Cantwell. On the large majority of issues, the language was the same or similar. Historically, major legislation often passes after substantial work in a previous Congress. That previous work settles much of the final package. Then, there are intense and often difficult negotiations on the final issues, which for privacy appear to be Federal preemption and private rights

of action. Nonetheless, however difficult those two issues may be, it is far easier to come to a final deal on two issues than to try to draft an entire bill on a blank slate.

2. *Industry and all those concerned about EU/U.S. relations have a strong interest in passing comprehensive Federal privacy legislation.* As just discussed above, there are compelling reasons why progress on U.S. privacy legislation would increase the possibility of a good outcome in the EU/U.S. negotiations. For the politically savvy companies that operate in both Europe and the United States, the benefit of supporting an overall U.S. law quite possibly outweighs any company-specific reasons to try to block the bill due to particular provisions in a privacy bill.
3. *Passage last month of the California privacy initiative provides business with a new, compelling reason to support Federal privacy legislation.* In November, the voters in California approved a ballot initiative, called the California Privacy Rights Act (CPRA), which goes into effect on January 1, 2023. The effective date, in my understanding, is no coincidence—it gives the 117th Congress time to complete action on a Federal law. CPRA, while having only mixed support from privacy and civil liberties advocates, would add new privacy restrictions, including in the area of online advertising. For this reason, online advertising companies and companies that buy online advertising have a new reason to support Federal legislation. Taken together with business support due to the EU situation, the U.S. business community in general is more prepared to accept broad national privacy rules than ever before.
4. *The California privacy initiative creates the possibility of greater agreement on Federal preemption.* To date, some members of this Committee have pushed for broad Federal preemption of state privacy laws, for reasons including preventing business from having to comply with multiple and possibly contradictory state laws. Other members of this Committee have pushed to have the Federal legislation be a floor but not a ceiling, allowing states to act first (as they have often done in the past) to enact greater protection of individual privacy. I have written three articles on preemption, about the *history* of Federal privacy preemption, identifying key *issues* for preemption, and a *proposal* (co-authored with Polyanna Sanderson of the Future of Privacy Forum) for a process to narrow disagreement, based on case-by-case examination of the numerous existing state laws.

   Building on this previous analysis, the recent passage of the CPRA creates a two-part proposal for how the differing sides on preemption can each achieve a substantial victory. First, as a win for those supporting privacy innovation in the states, the California Consumer Privacy Act, which went into effect already, would remain in effect. After all, businesses have already had to comply with that law, so the major costs associated with the law have already been spent. Second, the new Federal law could preempt the CPRA, which does not go into effect until 2023. Industry would thus be spared the challenge of re-engineering their data systems again, so soon after complying with CCPA. In addition, important privacy advocates, including the *ACLU of California* and the *Consumer Federation of California,* actually came out in opposition to CPRA. There may thus be an opportunity to reach agreement on a significant example of preemption. If both sides of this fierce debate win a significant victory, then there may be more room to address remaining preemption issues as something of a technical drafting matter.
5. *A Biden administration will support Federal privacy legislation.* The 2020 Democratic platform *calls* for enacting Federal privacy legislation, and the Obama administration supported privacy legislation as part of the 2012 *announcement* of a "Privacy Bill of Rights." Joe Biden himself has long worked on these issues. He spoke to the European Parliament in 2010, garnering headlines such as *this:* "Biden vows to work with EU parliament on data privacy." In addition, a Biden administration can draw on numerous individuals who have extensive government experience on privacy, including those who worked on the Privacy Bill of Rights and negotiated the Privacy Shield.
6. *The narrow majorities in both the Senate and House likely help define the scope of the possible for Federal privacy legislation.* As a resident of Georgia, I know only too well the intensity of effort for the two Senate run-off elections on January 5—my wife and I have basically given up answering our home telephone for the duration. After those run-offs, one of the parties will have a narrow working majority in the Senate, and the margin in the House of Representatives is also unusually narrow. With such narrow margins, bipartisan coopera-

tion will be at a premium—neither party can afford to support a privacy bill alone that would lose any of its members, so the clearest path to a majority is with bipartisan support. *Last year's proposals from the Senate Commerce Committee are the most logical starting point for negotiations.* New proposals from the wing of either party will likely have difficulty making it into the legislation, unless the proposals can garner support from a range of political viewpoints.

In conclusion on the prospects for Federal privacy legislation, the stars may finally have aligned to enact meaningful privacy protections. A new Federal privacy law would enshrine in law a considerable list of new privacy protections for individuals. The law would also have support from businesses who usually oppose new government regulation. *At a time when there is risk of partisan gridlock in Congress, Federal privacy legislation could be a significant instance of bipartisan accomplishment.*

Background of the witness:

Peter Swire is the Elizabeth and Tommy Holder Chair and Professor of Law and Ethics in the Scheller College of Business at the Georgia Institute of Technology. He is senior counsel with the law firm of Alston & Bird, and Research Director of the Cross-Border Data Forum.

In 1998, the Brookings Institution published Swire & Litan, "None of Your Business: World Data Flows, Electronic Commerce, and the European Privacy Directive. In 1999, Swire was named Chief Counselor for Privacy in the U.S. Office of Management and Budget, the first person to have U.S. government-wide responsibility for privacy policy. Swire was the lead White House official during negotiation of the EU/U.S. Safe Harbor.

After the Snowden revelations, Swire served as one of five members of President Obama's Review Group on Intelligence and Communications Technology, making recommendations on privacy and other reforms for the U.S. intelligence community. In 2015, the International Association of Privacy Professionals awarded Swire its annual Privacy Leadership Award. In 2016 he was an expert witness in the Irish trial for *Schrems v. Facebook,* and submitted testimony of over 300 pages describing the legal safeguards for the U.S. intelligence community's use of personal data.

In 2018, Swire was named an Andrew Carnegie Fellow for his project on "Protecting Human Rights and National Security in the New Age of Data Nationalism." In 2019, the Future of Privacy Forum honored him for Outstanding Academic Scholarship.

"Statutory and Non-Statutory Ways to Create Individual Redress for U.S. Surveillance Activities"

Appendix 1 to U.S. Senate Commerce Committee Testimony on "The Invalidation of the EU-U.S. Privacy Shield and the Future of Transatlantic Data Flows"

Peter Swire[1]

This document addresses a legal issue that calls for solution to enable continued lawful basis for flows of personal data from the European Union to the United States—individual redress. In *Schrems II,* the Court of Justice for the European Union held that the lack of individual redress in the United States for persons in the EU purportedly surveilled by U.S. intelligence was a basis for finding that the Privacy Shield, as approved by the EU Commission, did not provide "adequate" protection of personal data. In this setting, individual redress refers to the ability of an individual, including an individual in the European Union, to receive a determination that their rights have not been violated by U.S. national security surveillance.

For a U.S. audience, it is important to understand that the requirement of individual redress is a constitutional requirement, under Article 47 of the EU Charter of Fundamental Rights. The European Data Protection Board (EDPB) in November published the "*European Essential Guarantees"* based on the jurisprudence of the European Court of Justice and the European Court of Human Rights. One of the four essential guarantees, as described by the EDPB, is that "effective remedies

[1] Elizabeth and Tommy Holder Chair of Law and Ethics, Georgia Tech Scheller College of Business; Research Director, Cross-Border Data Forum; senior counsel, Alston & Bird LLP. The opinions expressed here are my own, and should not be attributed to the Cross-Border Data Forum or any client. For comments on earlier versions of the research, I thank Théodore Christakis, Dan Felz, Robert Litt, and Kenneth Propp. Errors are my own.

need to be available to the individual." This appendix to my December 9 testimony before

U.S. Senate Commerce Committee seeks to identify issues and suggest possible approaches to meet the individual redress requirement. The testimony for which this is an appendix contains a summary discussion of the issue of individual redress. This appendix provides more detailed analysis and legal citations, in hopes of advancing discussion of the individual redress issue.

This appendix to my testimony to the Committee has three sections:

1. Discussion of the proposal that I published on August 13 with Kenneth Propp, entitled "*After Schrems II: A Proposal to Meet the Individual Redress Problem.*" This article proposed ways that a new U.S. statute could apparently meet the EU legal standard for individual redress.
2. On October 14, European legal expert Christopher Docksey published *"Schrems II and Individual Redress—Where There's a Will, There's a Way."* This article found the Propp/Swire approach promising, while pointing out important aspects of EU law to be considered in any U.S. system for individual redress.
3. Discussion of non-statutory approaches for individual redress. Since August, working with others at the Cross-Border Data Forum, I have examined lawful ways to meet the goals of the initial proposal, in the event that Congress does not pass a new statute to do so.[2] This appendix includes a number of ideas that have not previously been published.

The discussion here necessarily addresses details of multiple areas of law, including constitutional, statutory, and administrative provisions of both U.S. and EU law, and including the complex legal provisions governing U.S. national security surveillance under the Foreign Intelligence Surveillance Act (FISA) and other laws. As Christopher Docksey emphasizes, the U.S. need not have perfect "equivalence" with EU law—in our different constitutional orders, there may not be any lawful way to provide precisely the same procedures as apply under the General Data Protection Regulation (GDPR) and EU fundamental rights law. Instead, the standard announced by the CJEU is "essential equivalence," a legal term that has been the subject of extensive interpretation by the CJEU. As EU courts have stated, the "essence of the right" must be protected. The effort here is to further the discussion of how such protections might be created under U.S. law.

I. Individual Redress Proposal Based on U.S. Statutory Change

On August 13, Kenneth Propp and I published in *Lawfare* "After *Schrems II:* A Proposal to Meet the Individual Redress Problem."[3] In that case, the CJEU observed that the U.S. surveillance programs conducted under Section 702 of the Foreign Intelligence Surveillance Act (FISA) or EO 12333 do not grant surveilled persons "actionable" rights of redress before "an independent and impartial court." The Court emphasized that "the very existence of effective judicial review designed to ensure compliance with provisions of EU law is inherent in the existence of the rule of law." It added that "legislation not providing for any possibility for an individual to pursue legal remedies in order to have access to personal data relating to him or her" fails to "respect the essence of the fundamental right to effective judicial protection," as set forth in Article 47 of the EU Charter of Fundamental Rights.

The CJEU identified two ways in which U.S. surveillance law lacks essential equivalence to EU safeguards. The first, and the focus of this article, is that the U.S. lacks an "effective and enforceable" right of individual redress. The second, which is beyond the scope of the proposal we offer here, is the finding that there is a lack of "proportionality" in the scale of U.S. intelligence activities. As discussed in the initial proposal, the CJEU thus measures U.S. surveillance law protections against an idealized, formal standard set forth primarily in EU constitutional law.

A. Lessons from ***Schrems II*** *About Redress*

The Privacy Shield was itself an iterative response to the criticisms of U.S. surveillance law voiced by the CJEU in striking down its predecessor, the Safe Harbor Framework, in 2015. In that *prior ruling,* the Court emphasized the importance of effective redress to protect surveilled persons, with an independent decision-maker providing protection for the individual's rights.

---

[2] Following the publication of the August proposal, I was asked by U.S. officials about the possibility of a non-statutory approach for individual redress. I then developed the non-statutory ideas that are published here for the first time, and described them to officials in response to their request.

[3] Kenneth Propp & Peter Swire, "After *Schrems II:* A Proposal to Meet the Individual Redress Problem."[3]

In response, the United States agreed in the Privacy Shield to designate an Ombudsperson, an Under Secretary of State, to receive requests from Europeans regarding possible U.S. national security access to their personal data, and to facilitate action by the U.S. intelligence community to remedy any violation of U.S. law. This role was built on top of the Under Secretary's previously assigned responsibilities under Presidential Policy Directive 28 as a point of contact for foreign governments concerned about U.S. intelligence activities. No change in U.S. surveillance law was needed to establish the Ombudsperson—only the conclusion of an interagency memorandum of understanding between the Department of State and components of the U.S. intelligence community.

In *Schrems II,* the CJEU disapproved of the Privacy Shield's Ombudsperson innovation. The Court observed that the Under Secretary of State was part of the executive branch, not independent from it, and in any case lacked the power to take corrective decisions that would bind the intelligence community. An inquiry conducted by an administrative official, with no possibility of appealing the result to a court, did not meet the EU constitutional standard for independence and impartiality, the CJEU held.

The implications of the CJEU's decision support the conclusion that any future attempt by the United States to provide individual redress, to meet EU legal requirements, must have two dimensions: (1) *a credible fact-finding inquiry* into classified surveillance activities in order to ensure protection of the individual's rights, and (2) *the possibility of appeal to an independent judicial body* that can remedy any violation of rights should it occur.

B. Possible Factfinders

In devising a system of individual redress for potential surveillance abuses, the first question is where best to house the fact-finding process. Our initial proposal mentioned two possible ways to conduct such fact-finding. The first is to task fact-finding to existing Privacy and Civil Liberties Officers (PCLOs) within the intelligence community, as established by *Section 803* of the Implementing Recommendations of the 9/11 Commission Act of 2007. The second is to enlist the Privacy and Civil Liberties Oversight Board, and independent agency tasked with oversight of intelligence community activities. Since we wrote the proposal, as discussed below, the suggestion has also been made that fact-finding could be carried out by the Office of the Inspector General in the relevant intelligence agency.

Beyond the question of whom in the U.S. Government is best-placed to act as a factfinder, a new system of individual redress would need to define the standard for that investigation. To meet the legal standard announced by the CJEU, the system would apply at least to individuals protected under EU law; the system might also enable actions for individual redress for U.S. persons. Precise definition will require the involvement of experts within the U.S. intelligence community as well as those knowledgeable about surveillance-related redress procedures in European countries. A legal standard for all complaints, at a minimum, would likely test compliance with U.S. legal requirements, such as whether collection under FISA Section 702 was done consistent with the statute and judges' orders governing topics such as targeting and minimization. In addition, a future agreement between the U.S. and the EU or other third countries could add provisions forming part of the investigative standard. For instance, as discussed below, there may be a way to state explicitly that the surveillance will be necessary and proportionate, which are important legal terms under the EU Charter of Human Rights and the European Convention on Human Rights. Our proposal noted that the U.S. might perhaps negotiate to ensure that the EU provide reciprocal rights for U.S. persons with respect to any surveillance conducted by EU Member States. Similarly, the new redress system might address other issues, including whether individuals would ever receive actual notice some period of time after they have been surveilled. Such notice has been an element of EU data protection law, although notice of intelligence activities appears to have been a rarity there in actual practice.

The fact-finding process would logically have two possible outcomes—no violation, or some violation that should be remedied. Where there is no violation, there would be a simple report to the individual, or perhaps to a Data Protection Authority acting in the EU on behalf of an individual. Under the Privacy Shield, the report was that there had been no violation of U.S. surveillance law or that any violation has been corrected. This sort of limited reporting about classified investigations exists for the U.K. Investigatory Powers Tribunal, which is *prohibited* from disclosing to the complainant "anything which might compromise national security or the prevention and detection of serious crime." As Christopher Docksey has noted, this type of reporting can also be found in Article 17 of the Law Enforcement Directive (EU) 2016/680.

Broader disclosure about classified investigations *risks* benefiting hostile states, terrorist groups or others. By contrast, where any violation is found, then no report could be given until the violation was remedied. For instance, if there was illegal surveillance about the person seeking redress, the personal data might be deleted or any other measure taken to remedy the violation.

C. Judicial Review in the FISC

In the initial article, we stated that the obvious and appropriate path for an appeal from the fact-finding stage would be to the Foreign Intelligence Surveillance Court (FISC). FISC judges, along with other Federal judges, meet the gold standard for independence, since Article III of the U.S. Constitution ensures that they have lifetime tenure and are located outside of the executive branch. Making the FISC responsible for the adjudication of individual complaints would go in some respects go beyond the FISC's current institutional responsibilities, but the Federal judges on the FISC are experienced in reviewing agency decisions in non-FISC cases. The FISC is better-suited than an ordinary Article III court would be, because of its specialized expertise in U.S. surveillance law and well-established procedures for dealing with classified matters. As discussed in more detail below, the FISC already provides judicial oversight for the FISA Section 702 program—and has a proven track record of effective oversight. In the wake of the Snowden revelations, numerous FISC decisions were declassified and made public. A detailed *review* of these decisions concluded: "The FISC monitors compliance with its orders, and has enforced with significant sanctions in cases of noncompliance."

A key legal issue in crafting such a system is ensuring that a plaintiff has "standing" to sue, as required by Article III of the U.S. Constitution. In the Irish High Court decision in *Schrems II,* Judge Costello *wrote* that "All of the evidence show that [standing] is an extraordinarily difficult hurdle for a plaintiff to overcome" in government surveillance cases. In summary, the plaintiff must show: (1) he or she has suffered injury in fact (2) that is causally connected to the conduct complained of and (3) is likely to be redressed by a favorable judicial opinion. Under EU law, an individual such as Max Schrems can bring a successful case without proving that he was ever under surveillance by the U.S. government. By contrast, as explained by *Tim Edgar* in *Lawfare,* plaintiffs in the U.S. have had to clear a high hurdle to establish standing and gain a legal ruling about the lawfulness of surveillance.

To assure standing for these appeals to the FISC, a mechanism similar to the one utilized under the U.S. Freedom of Information Act (FOIA) appears feasible. Under FOIA, any individual can request that an agency produce documents, without the need to first demonstrate particular "injury." The agency is then under a statutory requirement to conduct an effective investigation, and to explain any decision not to supply the documents. After the agency completes its investigation, the individual can appeal to Federal court to ensure independent judicial review. The judge then examines the quality of the agency's investigation to ensure compliance with law, and he or she can order changes in the event of any mistakes by the agency.

Analogously, when seeking individual redress on a matter relating to national security, the FISC could independently assess whether the administrative investigation met statutory requirements, and the judge could issue an order to correct any mistakes by the agency—including by correcting or deleting data or requiring additional fact-finding. This sort of judicial review of agency action is extremely common under the *Administrative Procedure Act* that applies broadly across Federal agencies. Typically, the judge must ensure that the agency action is not "arbitrary, capricious, an abuse of discretion, or otherwise not in accordance with law." There is standing on the part of the individual—a "case or controversy"—to assess whether the agency has properly discharged its statutory duties. As with FOIA, there is no need to determine whether the complaining individual has suffered injury in fact, since the statute creates a duty on the agency to act in a defined way.

We identify three features worth considering with this approach. First, due to the classified nature of the fact-finding, there may not be any workable way for the complainant to decide whether to bring an appeal. Therefore, it may make sense to have an automatic appeal to the FISC. Second, the 2015 USA FREEDOM Act established a role for appointed amici curiae who have full access to classified information and can brief the FISC on "legal arguments that advance the protection of individual privacy and civil liberties." These amici could play a role in advocating for the rights of the complainant, so that the FISC judge can receive briefing from both the agency and an amicus assigned to scrutinize the agency investigation. Third, Congress could consider whether the right to file a complaint be extended to U.S. persons in addition to those making complaints from the EU concerning surveillance under FISA Section 702 and EO 12333. Congress should consider how to structure a meaningful right to redress while avoiding a flood of complaints. The experience from *Eu-*

rope, and from prior agreements such as Privacy Shield and the Terrorist Finance Tracking Program, suggests that the actual number of complaints would likely be manageable.

II. Assessment by European Data Protection Expert Christopher Docksey

On October 14, Christopher Docksey published in *Lawfare* an article that commented on the Propp/Swire proposal, *"Schrems II and Individual Redress—Where There's a Will, There's a Way."* Docksey is a leading expert in EU data protection law, after a career as senior lawyer for the EU Commission and then Director and Head of Secretariat of the European Data Protection Supervisor.

Docksey was kind enough to state that "Propp and Swire's proposal provides a valuable framework for discussions by U.S. policymakers on a durable solution to individual redress in the United States." His objective was to respond to the proposal "from a European perspective, to underline the acceptable elements of their proposal and clarify which questions remain." He said: "The key to identifying potential points of future compromise by the EU is understanding the nature of three different types of institutions: "data protection officers (DPOs), independent supervisory authorities (DPAs) and courts."

A. Fact-Finding Phase

For the fact-finding phase, we suggested either the Section 803 Privacy and Civil Liberties Officers (PCLOs) or the PCLOB. Docksey explored having the fact-finding conducted either by the Office of Inspector General (OIG) or else the PCLOB.

In assessing the PCLOs, Docksey compares them to DPO's, whom he describes as "part of the organization of the data controller but have the right and duty to act independently in carrying out their roles." Because they are within the organization itself—the Federal agency—Docksey concludes they do not meet the EU requirement of "independent oversight."

Docksey examines the role of the OIG, and concludes: "It could be useful to explore whether the powers of the inspectors general could be strengthened to hear complaints referred by PCLOs and adopt binding orders for corrective action." As a potentially important factor for the EU legal analysis, OIG's have a reporting relationship to Congress—outside of the agency itself. As a legal risk of deploying the OIG's, Docksey observes that an Inspector General "can be easily removed, as recent experience shows."

Under Docksey's analysis, the PCLOB, as an independent agency, is most similar to the European institution of the data protection authority. As shown in a report by the EU Fundamental Rights Agency, national law in the EU varies in the manner of supervision. Some nations enable their usual DPA's to have oversight for national security investigations. Others, such as the Netherlands, have independent supervisory agencies specifically for intelligence activities. Docksey underscores the EU legal requirement of the right to independent supervision by a DPA, which "is enshrined as a specific element of the right to protection of personal data in Article 8(3) of the EU Charter and in Article 16(2) of the EU Treaty itself."

Assuming that the PCLOB has legal authority to conduct the investigation, therefore, the most analogous U.S. institution to a DPA, for conducting the fact-finding, would be the PCLOB. Concerning legal authority, the statute creating the PCLOB specifically provides that it shall have the power to review and analyze actions the Executive Branch takes to protect the U.S. from terrorism. The PCLOB's actions, however, have not been limited only to terrorism-related activities. As shown on the agency's *website,* the PCLOB has taken additional actions, including under Executive Order 13636 on Improving Critical Infrastructure Cybersecurity, as well as a request from the President that the Board provide an assessment of implementation of Presidential Policy Directive 28 (PPD–28), concerning protection of privacy and civil liberties in U.S. signals intelligence activities. By statute, Congress could explicitly authorize a role for the PCLOB in the individual redress process. As discussed further below, even in the absence of a statute, there would appear to be a legal basis for the PCLOB to play a role in a new individual redress process.[4]

In conclusion on the fact-finding phase, there are multiple possible ways to create the independent fact-finding process required under EU law. In addition, as Docksey

[4] The PCLOB has a staff that is small compared to employment by U.S. intelligence agencies, so a problem might arise if there are many requests for individual redress. In response, first, my understanding is that there was only one request to the Privacy Shield Ombudsman in the five years that the position existed, so staffing may not be a problem. In addition, the agency may be able to assist the PCLOB in the fact-finding, such as by "detailing" agency individuals to work on behalf of the PCLOB. This sort of "detailing" has often been used in the Federal government where expertise and staffing exist in one agency, but individuals are temporarily placed under the direction of the White House or a different agency.

explains in detail, the EU legal standard is not "absolute equivalence"; instead the U.S. must provide "essential equivalence" to EU legal protections. Docksey in his article explains reasons, in his view, why some U.S. approach to individual redress could indeed meet this "essential equivalence" standard.

B. Judicial Review in the FISC

Once the fact-finding phase is complete, Docksey emphasized the constitutional requirement, under EU law, for judicial review. Article 47 of the EU Charter states the constitutional text—there must be a right to an "effective remedy before a tribunal."

In the *Schrems II* case, as quoted by Docksey, "the advocate general enumerated the criteria laid down by the CJEU to assess whether a body is a tribunal." The advocate general wrote that the decision hinges on "whether the body is established by law, whether it is permanent, whether its jurisdiction is compulsory, whether its procedure is inter partes, whether it applies rules of law and whether it is independent[.]" Docksey adds: "Probably the most important of these criteria is the requirement of independence. This means acting autonomously, without being subject to decisions or pressure by any other body that could impair the independent judgment of its members."

The FISC is a close fit for these announced criteria for judicial review:

1. *Independence.* For the most important criterion, each FISC judge meets the gold standard for independence. Decisions are made by a judge nominated by the President and confirmed by the Senate. Each judge has lifetime tenure, and cannot be removed except under the historically rare process of impeachment in the Congress.
2. *Established by law and applies rules of law.* The FISC is established by law in the Foreign Intelligence Surveillance Act (FISA) and other statutes. It applies rules of law, including these statutes and its published *rules of procedure.*
3. *Permanence.* The FISC is permanent, in the sense that the authorizing statutes continue in operation unless there is a new statute passed by the Congress.
4. *Compulsory jurisdiction.* The FISC is a Federal court, established under Article III of the U.S. constitution. A Federal judge acting in the FISC has the same judicial powers as a Federal judge operating generally in the Federal courts. For instance, the judge issues a binding order, punishable by contempt of court, in cases of non-compliance. As with Federal judges generally, the binding order can apply to a Federal agency as well as to individuals.
5. *Procedure "inter partes."* The FISC originally acted *ex parte,* without opposing counsel, and now has procedures to act "*inter partes,*" with counsel in addition to the government. The Review Group on Intelligence and Communications Technology *explained* in 2013 the reason for this change:

   "When the FISC was created, it was assumed that it would resolve routine and individualized questions of fact, akin to those involved when the government seeks a search warrant. It was not anticipated that the FISC would address the kinds of questions that benefit from, or require, an adversary presentation. When the government applies for a warrant, it must establish 'probable cause,' but an adversary proceeding is not involved. As both technology and the law have evolved over time, however, the FISC is sometimes presented with novel and complex issues of law. The resolution of such issues would benefit from an adversary proceeding."

   Consistent with this recommendation, Congress created a set of *amici curiae,* experts in privacy and related matters, in the USA FREEDOM Act of 2015. *50 U.S.C. § 1803(1)(i).* A judge in the FISC "may appoint an individual or organization to serve as amicus curiae, including to provide technical expertise, in any instance as such court deems appropriate." As part of any negotiation with the EU, the U.S. government could consider promising to request appointment of such an amicus curiae in any case involving the rights of an EU person. With such an appointment, the FISC would meet the EU criterion of procedure *inter partes.*

In conclusion on the Docksey article, the discussion here has indicated options, consistent with EU law, for fact-finding concerning a complaint by an EU person about a possible violation of rights. Appeal then could be to the FISC, which meets the EU legal criteria for a "tribunal." Docksey himself, after completing his analysis of the proposal, concluded: "It is time to grasp the nettle. A compromise is worth the effort. And if there is the will, there is a way."

III. Non-Statutory Variations on the Proposals

Since our proposal was published in August, it has become more urgent to consider ways to establish an individual redress procedure without necessarily awaiting a statute passed by the Congress, for at least three reasons:

1. Drafting a statute on these novel issues is a complex task, which even with full agreement among members of Congress could take substantial time to complete.
2. The possibility has grown that there may soon be large cut-offs of personal data from the EU to third countries such as the U.S. As Professor Théodore Christakis has recently *explained,* the November guidance from the European Data Protection Board appears to conclude that it is illegal, for a very wide array of routine business practices, to transfer personal data from the EU to third countries.
3. Non-statutory approaches are worth considering even if a somewhat better system might be created by a statute. A non-statutory approach quite possibly is the best way to ensure that data flows and privacy protections exist during an interim period while legislation is being considered. Drafting a non-statutory approach can benefit from commentary from experts in the U.S. and EU legal systems, and the U.S. and EU officials working on the issue can identify and address nuanced issues about how to meet legal and policy goals for an agreement. In short, a non-statutory approach may be sufficient long-term to provide individual redress by non-statutory means, although European law emphasizes the strength of protections memorialized in a statute. Alternatively, a non-statutory approach might bridge the period until Congress enacts a statute.

As with Parts I and II above, the discussion here addresses the fact-finding phase and then the possibility of judicial review.

A. Fact-finding Phase

The discussion here of the Docksey article mentioned possible roles in fact-finding for the Section 804 Privacy and Civil Liberties Officers in each agency, the agency Inspectors General, and the PCLOB. The analysis here suggests possible ways that each might play a role in fact-finding without statutory change.

The Section 804 PCLO's are subject to an Executive Order or similar mandates from the President. As a general matter, an Executive Order, Presidential Policy Directive, or other executive action can take effect under the President's power under Article II of the U.S. constitution to "take care" that the laws are faithfully executed. For national security matters, the President also can act as Commander-in-Chief. Expertise in the possible scope of executive power resides in the Office of Legal Counsel in the U.S. Department of Justice, working with White House Counsel and other officials. As one example, the PCLO's could be ordered by the President to cooperate in specified ways with others involved in fact-finding, such as the PCLOB.

As Docksey notes, there is a strong tradition of reporting from the Inspectors General to Congress, and IG's have a history of independence, in order to investigate and report on the agencies within which they reside. There may be ways by Executive Order or other executive action to strengthen IG independence, as Docksey suggests may be required by EU law.

As discussed above, the PCLOB plays the role of independent supervisory agency most closely analogous to the supervisory agencies that exist in the EU. Due to its independence, I am not sure the extent to which the PCLOB would be bound by an Executive Order or other presidential action. Nonetheless, one promising approach would be if the PCLOB entered into a legally-binding Memorandum of Understanding (MOU) with an Executive Branch agency. This MOU would be a public commitment by the PCLOB and the Executive Branch agency to act in agreed-upon ways to conduct fact-finding. To the extent that the EU has questions about the legal enforceability in court of such an MOU, any agreement with the U.S. leading to adequacy could be conditional on the MOU remaining in force. As with other adequacy determinations, the EU would periodically assess how procedures are working in practice, and the EU could therefore withdraw its adequacy finding if the MOU were not followed.

In conclusion on the fact-finding phase, there would appear to be considerable scope for executive action and/or agreements between agencies to put in place effective fact-finding mechanisms for individual redress. Drafting of such measures can be informed by the insights offered by Christopher Docksey in his articles, and from other experts.

B. Judicial Review by the FISC

As described in the Propp/Swire proposal, Congress can provide by statute for an appeal to go to the FISC. The discussion here suggests a legal approach, without the need for a statute, that may also enable appeal to the judges in the FISC. The basic idea is that the U.S. Government could request review by the FISC, as part of the court's inherent authority to review implementation of its Section 702 orders. The U.S. Government could promise, such as in an agreement with the EU, that it will petition the FISC to review each complaint under the redress system in this manner. As a result, independent Federal judges would provide judicial review of the complaints, and have authority to issue binding orders in the event of violations.

The approach discussed here has not been published previously, so I offer it as an initial public draft, with relatively detailed citations to relevant authorities.

1. FISC Oversight of Section 702 Orders

The proposed approach would build on existing FISC supervision of national security surveillance. Judges in the FISC issue binding legal orders about how requirements apply for any surveillance under Section 702. FISC authorizes Section 702 surveillance each year by entering an order that evaluates the conduct of the 702 program over the past year, imposes new restrictions or requirements as appropriate, and approves targeting, querying, and minimization procedures for U.S. intelligence agencies. *50 U.S.C. § 1881a(j)(3)* (requiring FISC to "enter an order" authorizing 702 program if government's annual certification meets statutory and constitutional requirements); *see also, e.g.,* In re Government's Ex Parte Submission of Reauthorization Certifications and Related Procedures, Case caption redacted (Foreign Int. Surv. Ct. Dec. 6, 2019), *available here* (order authorizing 2019 Section 702 intelligence programs).

In the U.S. legal system, Federal judges have "inherent authority" under Article III of the Constitution to take judicial action in order to ensure compliance with judicial orders. FISC has Article III authority. *See, e.g.,* In re: Certification of Questions of Law to the Foreign Intelligence Court of Review, No. FISCR 18–01, at 8 (FISA Ct. Rev. Mar. 16, 2018), *available here* ("FISC's authority . . . is cabined by—and consistent with—Article III of the Constitution). Further, FISA expressly ensures FISC can exercise this authority in regards to FISC's own orders, *stating* that "[n]othing in [FISA] shall be construed to reduce or contravene the inherent authority of [FISC] to determine or enforce compliance with an order or . . . a procedure approved by [FISC]."

Under the proposed approach, the U.S. Government would essentially ask the FISC to do no more than exercise its inherent authority as an Article III court, to review that 702 intelligence activities conducted in regards to a specific individual complied with the FISC's own 702 authorization order and applicable law.

This approach would fit with FISC's general monitoring of the intelligence community's compliance with its orders and U.S. surveillance laws. The FISC Rules of Procedure already require the government to report any noncompliance with a FISC order. *See* FISC Rule of Procedure 13(b) (requiring the government to report all cases where "any authority or approval granted by [FISC] has been implemented in a manner that did not comply with [FISC's] authorization or applicable law"). The FISC itself has not hesitated to monitor and, if warranted, aggressively enforce compliance with its orders. Examples include the FISC's questioning the NSA's compliance with FISC orders governing the post-9/11 Internet metadata program, ultimately leading to the program's termination, or the FISC's more recent orders requiring the government to respond to the DOJ Inspector General's findings relating to the Carter Page and other FISA warrant cases, both of which are discussed in Appendix 2 to today's testimony.

Put another way, this approach fits well within the joint, ongoing system of oversight for 702 surveillance that the FISC and the U.S. Government already work together to provide. The Government subjects 702 surveillance to a range of oversight mechanisms, including day-to-day supervision within intelligence agencies, supervision by the Oversight Section in DOJ's National Security Division (NSD), and regular joint on-site audits of 702 surveillance by NSD and ODNI. *See, e.g.,* Joint Unclassified Statement to the H. Comm. on the Judiciary, 114th Cong. 4 (2016), *available here.* Existing FISC orders also require the government to report violations of 702 authorization orders. *See PCLOB 702 Report* at 29–30 (referencing a still-classified 2009 FISC opinion imposing reporting requirements). All compliance incidents identified through these processes are reported to the FISC. The FISC reviews these compliance incidents as part of its annual 702 reauthorization. This review can give rise to FISC requiring remediation or imposing new restrictions on intelligence activities in its 702 authorization orders.

The approach also seems to fit within procedural, jurisdictional, and national-security constraints under which the FISC operates:

- *The U.S. Government is entitled to ask FISC for relief.* The FISC Rules of Procedure generally require "the government" or "a party" to file pleadings requesting relief from FISC. *See, e.g.,* FISC Rules of Procedure 6(a)-(b) (permitting "the government" to request certain relief); 6(c)-(d) (permitting "a party" to request certain relief); 19(a) (permitting "the government" to file show-cause motions); 62(a) (permitting "a party" to move for publication of FISC decisions). If an individual were to file a petition with the FISC, this could give rise to questions about whether she is "a party" entitled to request relief. But it would seem clear that a motion from the U.S. Government would be from "the government" as contemplated under FISC rules.
- *The U.S. Government should not face standing hurdles.* When non-governmental parties have requested relief from FISC in the past, FISC has required them to plead Article III standing. *See, e.g.,* In re Opinions & Orders of this Court Addressing Bulk Collection of Data under [FISA], Misc. 13–08 (Foreign Int. Surv. Ct. Nov. 9, 2017), *available here* (chronicling litigation over whether ACLU had Art. III standing to request that FISC publish orders relating to Section 215 programs). In contrast, the U.S. Government is already entitled to obtain 702 authorization orders from FISC in *ex parte* proceedings, without needing to show standing. The Government should thus also be able to ask FISC to review and enforce compliance in connection with those same 702 orders.
- *National security interests remain protected.* In recent decisions, the FISA Court of Review has reasserted the FISC's "unique" national-security need to maintain secrecy. *See, e.g., In re: Certification of Questions of Law to the Foreign Intelligence Court of Review,* No. FISCR 18–01, at 3 (FISA Ct. Rev. Mar. 16, 2018), *available here* (emphasizing that "[t]he very nature of [FISC's] work . . . requires that it be conducted in secret," and that FISC orders "often contain highly sensitive information" whose release "could be damaging to national security"). The proposed approach would not require FISC to disclose classified information, or otherwise impair the secrecy under which FISC normally operates.

2. What would the FISC Review?

A non-statutory proposal would need to define the scope of oversight the FISC can and would review. The statutory text of Section 702 states that the FISC oversees the targeting, querying, and minimization procedures of intelligence agencies. Based on that text, the FISC would have oversight at least over those procedures, but perhaps not more broadly. The EU potentially could seek very broad oversight, along the lines of "full compliance with all the rights of a data subject" under EU law. Defining the scope of oversight would quite possibly be an important subject of negotiation between the U.S. and EU.

Scope of FISC's subject-matter jurisdiction. The FISC can only operate within its subject-matter jurisdiction. Recent decisions of the FISA Court of Review have discussed the FISC's defined subject-matter jurisdiction, which may prevent non-parties from requesting relief that merely "relates to the FISC or the FISA," as opposed to relief expressly authorized by FISA. *See, e.g., In re Opinions & Orders by the FISC Addressing Bulk Collection of Data under [FISA],* FISCR 20–01 at 18–19 (FISA Ct. Rev. Apr. 24, 2020), *available here* (holding FISCR did not have subject-matter jurisdiction to adjudicate ACLU request to declassify portions of Section 215 orders). The proposed approach, however, would merely ask FISC to confirm compliance with its own orders, which FISA expressly authorizes FISC to do.

Possibly build agreement with the EU into the scope of the targeting, querying, and minimization procedures. One potentially fruitful path is to include EU-relevant provisions in the annual authorizations by the FISC of Section 702. For instance, the targeting procedures might adopt language responsive to EU legal concerns, such as stating that targeting shall be done only as necessary and proportionate. If the FISC order concerning 702 required necessity and proportionality—key terms within EU law—then the FISC presumably could oversee implementation of those necessity and proportionality requirements. The U.S. Government would have the ability to request such language, or other language negotiated with the EU, in the targeting procedures, as part of its regular legal submissions to the FISC. The FISC could issue binding requirements on U.S. agencies to ensure compliance with its Section 702 orders.

Due to the defined subject matter jurisdiction of the FISC, the court quite possibly would not have judicial authority to rule on the legality of surveillance under EO 12,333. The FISC review above is predicated on the FISC's authority to oversee im-

plementation of Section 702 orders, but the FISC has no similar statutory authority over an executive order, such as EO 12333.

I offer five observations about EO 12,333:

- First, the *fact-finding phase,* potentially including intelligence agencies and the PCLOB, *could apply to both Section 702 and EO 12,333.* Perhaps legal theories could be developed about how the FISC could review, as an ancillary matter, the portion of the record pertaining to EO 12,333. My tentative conclusion, however, is that review of EO 12,333 surveillance would be outside of the scope of the FISC's authority, absent statutory change.
- Second, *EO 12,333 surveillance may be sufficiently protected by the procedural steps before the complaint gets to the FISC.* The PCLOB or an agency procedure, for instance, could be the final arbiter on EO 12,333 issues. Docksey specifically presents arguments about why a PCLOB decision might meet EU legal requirements.
- Third, the *Commerce Department White Paper contains multiple arguments about why no further legal protections should be required* for companies using standard contractual clauses. Importantly, for instance, the White Paper states that it is unclear how companies can "consider any U.S. national security data access other than targeted government requirements for disclosure such as under FISA 702." Under these approaches, the U.S. government has thus articulated reasons why the scope of individual redress should match Section 702, rather than including EO 12,333.
- Fourth, in practice, many companies are addressing EO 12,333 by taking additional safeguards with respect to *secure communications* when personal data leaves the EU, such as to come to the U.S. There is ongoing discussion among European actors about the extent to which use of strong encryption answers EU legal concerns about EO 12,333 surveillance. If such use of encryption turns out to meet EU legal requirements, then individual redress can apply to the cases where it is relevant, under Section 702.
- Fifth, and if the previous observations do not apply, I present as another possible approach the following analysis of why an effective regime of individual redress may meet the EU legal standard of "*essential equivalence,*" even if EO 12,333 is outside of that regime. In recent cases concerning data retention, the CJEU highlighted its jurisdiction where a government achieves surveillance via private actors, such as companies subject to a judicial order. By contrast, the CJEU did not say that it had jurisdiction, in the face of the national security exception to its jurisdiction, where a government performs surveillance directly (not through a private company). Judicial orders to private companies apply to Section 702, but not to government activities under EO 12,333. With the disclaimer that I am a U.S. lawyer, perhaps it is worth considering whether the EU "essentially equivalent" regime of individual redress, to that offered by the EU Member States, might apply only to judicially ordered actions by companies, that is, to Section 702. With the same disclaimer, the same limit on "national security" jurisdiction does not apply to the European Court of Human Rights, and potentially its jurisprudence would apply to the direct government actions under EO 12,333.

Conclusion

This document has attempted to set before this Committee and the public research to date about how to create a system of individual redress under U.S. law. Standing doctrine, under Article III of the U.S. constitution, can block many proposed ideas for offering individual redress to an individual. The Propp/Swire proposal explained how the analogy to FOIA can require an agency to act, with a court then empowered to review the agency action. Christopher Docksey has supplemented the initial proposal with his expert insights about EU legal requirements. The new discussion here then presents ways that valid individual redress might be created by the U.S. government, even before Congress is able to enact a statute.

Members of this Committee and other U.S policymakers may doubt whether it is desirable as a policy matter to create such systems of individual redress for EU citizens. In response, there is this simple point—the highest court of the European Union has stated, apparently as a matter of its constitutional law, that such individual redress is required. Absent a valid system of individual redress, any future agreement between the U.S. and EU will be subject to great risk of invalidation. Faced with that reality, the proposals here seek to present possible solutions. Creative alternative proposals are most welcome, and the task is important.

"UPDATES TO U.S. FOREIGN INTELLIGENCE LAW SINCE 2016 TESTIMONY"

APPENDIX 2 TO U.S. SENATE COMMERCE COMMITTEE TESTIMONY ON "THE INVALIDATION OF THE EU-U.S. PRIVACY SHIELD AND THE FUTURE OF TRANSATLANTIC DATA FLOWS"

Peter Swire[1]

This Appendix supplements written testimony I am submitting to the Senate Committee on Commerce, Science, and Transportation for the December 9, 2020 hearing on "The Invalidation of the EU–U.S. Privacy Shield and the Future of Transatlantic Data Flows." This Appendix presents updates on the U.S. legal and regulatory regime for foreign intelligence surveillance that have occurred since testimony I provided to the Irish High Court in 2016 on the same subject (the "2016 Testimony").[2] Taken together, the 2016 Testimony and this Appendix seek to present an integrated set of references that may inform ongoing assessments, under European Union law, of the adequacy of protection of personal data related to U.S. foreign intelligence law.

My 2016 Testimony was submitted in November 2016, several months after the EU Commission adopted the finalized Privacy Shield in July 2016. At that time, I listed over twenty significant privacy-protective changes that had been made to U.S. foreign intelligence laws since the Snowden disclosures in 2013.[3] My 2016 Testimony then discussed the systemic safeguards present in U.S. law for foreign intelligence, including: (a) safeguards anchored in the statutes governing foreign intelligence surveillance by U.S. agencies,[4] (b) interlocking executive, legislative, and independent oversight mechanisms that are in place for surveillance activities;[5] (c) transparency mechanisms implemented since the Snowden disclosures that offered a level of transparency into U.S. surveillance practices unparalleled in other nations;[6] and (d) privacy safeguards implemented within the Executive Branch to protect personal information of non-US persons.[7] Chapter 5 of my 2016 Testimony also contained a detailed discussion of declassified opinions of the Foreign Intelligence Surveillance Court (FISC), including my assessment that the FISC has exercised careful and effective oversight over foreign intelligence surveillance.[8]

This Appendix highlights updates that have occurred since the 2016 period in which Privacy Shield and my Testimony was finalized. As an overview of what will be discussed in this Appendix, the following represents a summary of intervening developments that have resulted in greater safeguards, or the continued effectiveness of safeguards in place, since the 2016 period in which Privacy Shield and my prior Testimony were finalized:

1. The FISA Amendments Reauthorization Act of 2017 (FARA) introduced new safeguards for Section 702 programs, including:
   (a) mandating querying procedures for 702-acquired information,
   (b) codifying the National Security Agency (NSA) and Federal Bureau of Investigation (FBI) practice of appointing Privacy and Civil Liberties Officers,
   (c) expanding whistleblower protections to Intelligence Community (IC) contractors,
   (d) increasing disclosure and transparency requirements for Section 702 programs, and
   (e) imposing significant restrictions on the recommencement of Abouts collection.

---

[1] Elizabeth and Tommy Holder Chair of Law and Ethics, Georgia Tech Scheller College of Business; Research Director, Cross-Border Data Forum; senior counsel, Alston & Bird LLP. The opinions expressed here are my own, and should not be attributed to the Cross-Border Data Forum or any client. For research assistance on this appendix I thank Daniel Felz and Sara Guercio. This Appendix is based on publicly available information; I have not had access to any relevant classified information since 2016. The views expressed here are my own.

[2] PETER SWIRE, TESTIMONY OF PETER SWIRE (submitted to High Court of Ireland Nov. 3, 2016), available at *https://www.alston.com/en/resources/peter-swire-irish-high-court-case-testimony/*.

[3] *See id.* at 3–10—3–12.

[4] *See id.* at 3–12—3–26.

[5] *See id.* at 3–26—3–34.

[6] *See id.* at 3–34—3–38.

[7] *See id.* at 3–39—3–49.

[8] *See id.* at 5–1—5–53.

2. The FISC has continued to annually evaluate Section 702 surveillance as required under Section 702, and its reauthorization orders have resulted in new protections for Section 702 programs.
3. As a result of FISC's continued supervision of Abouts collection the NSA (a) voluntarily terminated Abouts collection and (b) segregated and deleted all Internet transactions previously acquired through its Upstream program.
4. The Office of Director of National Intelligence (ODNI) has continued to declassify significant documents relating to Section 702 surveillance, such as publishing the Section 702 trainings that NSA provides to its internal personnel that conduct Section 702 programs on a day-to-day basis.
5. Due in part to compliance incidents reported to the FISC, NSA decided to delete three years' worth of Call Detail Records (CDRs) obtained under the USA FREEDOM Act. NSA then decided to suspend its CDR program in early 2019.
6. The Privacy and Civil Liberties Oversight Board (PCLOB) issued new oversight reports on (a) the NSA's Call Detail Records program under the USA FREEDOM Act, as well as (b) the implementation of Presidential Policy Directive 28 (PPD–28) in U.S. intelligence agencies. PCLOB also recently announced it concluded an oversight review of the U.S. Treasury Department's Terrorist Finance Training Program.[9]
7. The ODNI has continued to publish annual Statistical Transparency Reports showing numerical statistics that provide transparency on the extent to which U.S. agencies are requesting data under FISA authorities, including Section 702 authorities.
8. The Department of Justice (DOJ) and ODNI continue to publish Semiannual Reports on the NSA's, FBI's, and CIA's compliance with Section 702 requirements, including statistics and descriptions of instances of non-compliance. These Reports continue to be created as a result of DOJ/ODNI's regular onsite reviews of the intelligence agencies.
9. U.S. foreign intelligence law continues to permit companies to publish transparency reports. My review of leading technology companies' recent transparency reports shows that, as in 2016, U.S. intelligence appears to affect a vanishingly small percentage of their active users.
10. ODNI has continued to publish significant quantities of declassified documents related to U.S. foreign intelligence activities on the "IC on the Record" website. It also facilitated greater access to these documents by launching a text-searchable capability on Intel.gov.
11. FISC has continued to declassify opinions and publish statistics on its handling of government surveillance applications. The percentage of applications that the FISC has modified or denied has increased since 2016.

This Appendix discussed the above developments in eight Sections that track the structure of my 2016 Testimony: 1) updates to systemic safeguards for U.S. foreign intelligence, 2) updates to Section 702 programs, 3) updates to the former 215 program, 4) updates to oversight safeguards, 5) updates to transparency safeguards, 6) updates to executive safeguards, 7) updates to Foreign Intelligence Surveillance Court (FISC) testimony, 8) updates to surveillance-related standing cases.

1. Updates to Systemic Safeguards for U.S. Foreign Intelligence:

A significant portion of my 2016 Testimony discussed the systemic safeguards built into the structure of foreign intelligence in the United States.[10] The core and structure of these safeguards has remained unchanged since I testified in 2016. The U.S. remains a constitutional democracy committed to the rule of law in conducting

[9] *See generally* U.S. Privacy and Civil Liberties Oversight Bd., *Press Release: Privacy and Civil Liberties Oversight Board Concludes Review of Treasury Department's Terrorist Finance Tracking Program,* (Nov. 19, 2019) available at *https://documents.pclob.gov/prod/Documents/EventsAndPress/de7972f6-03f1-48fd-8acd-b719a658e4a0/TFTP%20Board%20Statement.pdf.* PCLOB Chairman Adam Klein also issued a statement describing EU decisions to rely on TFTP instead of building its own equivalent program, and identifying privacy protective measures in place for EU citizens within TFTP, such as storage of EU bank customer data in the EU. *See* U.S. Privacy and Civil Liberties Oversight Bd., *Statement by Chairman Adam Klein on the Terrorist Finance Tracking Program,* (Nov. 19, 2020) available at: *https://documents.pclob.gov/prod/Documents/EventsAndPress/b8ce341a-71d5-4cdd-a101-219454bfa459/TFTP%20Chairman%20Statement%2011_19_20.pdf.*

[10] *See generally* SWIRE, *supra* note 2 at 3–2—3–49.

foreign-intelligence surveillance.[11] Further, U.S. surveillance remains subject to an interconnected system of statutory safeguards,[12] oversight mechanisms,[13] transparency mechanisms,[14] and Executive Branch safeguards.[15] My detailed discussion of these safeguards can be read in my 2016 Testimony, as outlined in the introduction above.

2. Updates to Section 702 Programs.

Section 702 of FISA is the basis for significant foreign intelligence collection by U.S. intelligence agencies, and was discussed at length in my 2016 Testimony.[16] Since 2016, the legal structure of Section 702 has remained largely unchanged. Section 702 requires the Attorney General and DNI to annually apply to the Foreign Intelligence Surveillance Court (FISC) to authorize Section 702 surveillance programs.[17] In doing so, the FISC reviews and authorizes the targeting, minimization, and (since 2018) querying procedures under which the intelligence agencies conduct Section 702 surveillance.[18] Throughout the ensuing year, the agencies' conduct of Section 702 programs is monitored by internal procedures, external audits, and regular reporting to the FISC and Congress.[19] The primary programs that exist under Section 702 remain (a) the Prism program, in which agencies such as the NSA serve directives on communications providers compelling the disclosure of communications to or from a tasked selector; and (b) the Upstream program, in which Internet backbone providers acquire communications to or from a tasked selector as they traverse the Internet.[20] My 2016 Testimony discusses the structure of Section 702 as well as its primary programs in detail.[21]

Despite broad continuity in Section 702 practice since my 2016 Testimony, a number of significant updates have occurred. This Section briefly summarizes a selection of these changes: (a) the FISA Amendments Act Reauthorization Act of 2017 and its privacy-protective aspects; (b) the FISC continues to reauthorize the Section 702 programs annually; (c) NSA terminated Upstream's Abouts collection in connection with 2017 FISC Reauthorization; (d) statistics on 702 programs continue to be released by the U.S. government; (e) the U.S. government continues to publish the Semiannual Assessment of compliance for 702 programs; and, (f) NSA declassified its internal guidance and training manuals for 702 programs.

a. FISA Amendments Reauthorization Act of 2017 (FARA)

In 2018, the FISA Amendments Reauthorization Act of 2017 (FARA) was passed, reauthorizing FISA for a five-year term and providing additional oversight and privacy protections.[22] Specifically, FARA i) mandated that intelligence agencies adopt querying procedures governing how they may access and use Section 702 intelligence; ii) codified the appointment of Privacy and Civil Liberties Officers in the NSA and FBI; iii) expanded whistleblower protections; iv) increased agency disclosure requirements; and v) required an approval process if the NSA wishes to restart Abouts collections.[23]

i. Mandatory Querying Procedures

Before FARA, Section 702 mandated that intelligence agencies adopt "targeting" and "minimization" procedures, which collectively provided the standards by which individuals are targeted for foreign intelligence surveillance and how subsequently acquired communications may be retained and used. FARA added a requirement that the NSA, FBI, CIA, and NCTC adopt "querying" procedures governing how these agencies are permitted to access and search 702-acquired communications.[24] Like targeting and minimization procedures, Section 702 querying procedures must be annually submitted to the FISC for approval, and FISC must evaluate them for consistency with FISA and "the requirements of the Fourth Amendment."[25] While

---

[11] *See id.* at 3–2—3–6.
[12] *See id.* 3–12—3–26.
[13] *See id.* at 3–26—3–34.
[14] *See id.* at 3–34—3–38.
[15] *See id.* at 3–39—3–49.
[16] *See id.* at 3–18—3–24.
[17] *See id.* at 3–18—3–21.
[18] *See id.*
[19] *See generally id.*at 3–2—3–49.
[20] *See generally id.*at 3–18—3–24.
[21] *See id.*
[22] *See* FISA Amendments Reauthorization Act of 2017, Pub. L. 115–118, (2018) [*hereinafter* "FARA"].
[23] *See generally id.*
[24] *Id.* § 101.
[25] *Id.* § 101(a)(1)(B)(f)(1) (2018).

FARA set forth specific requirements for U.S. person queries,[26] the querying procedures adopted by U.S. intelligence agencies contain safeguards for all individuals regardless of nationality. For example, the NSA's 2019 Querying Procedures state that "[e]ach query of NSA systems containing unminimized content or noncontent information acquired pursuant to section 702 . . . must be reasonably likely to retrieve foreign intelligence information."[27] These requirements, and FISC's annual review of how they are followed by U.S. intelligence agencies, help support proportional use of communications acquired under Section 702.

ii. Ratification of Appointment of PCLOs within Agencies

Under its Section 109, FARA expressly required the NSA and FBI to appoint Privacy and Civil Liberties Officers (PCLOs).[28] This change represented more of a change in law than in practice, since both NSA and FBI already had active PCLOs in place as a matter of internal policy before FARA was enacted.[29] Nonetheless, FARA's express codification of NSA's and FBI's prior practice represents Congress's approval of the IC practice of installing oversight and privacy protection offices directly within the agencies that conduct foreign intelligence surveillance.

iii. Expansion of Whistleblower Protections

FARA extended available whistleblower protections to contract employees working within U.S. intelligence agencies.[30] Prior to FARA, "contractors were protected from agency management retaliation," but not from retaliation from the contractor's direct employer.[31] FARA thus extended whistleblower protections to prohibit retaliation against a whistleblowing IC contractor by the contractor's employer.[32] As a result, IC contractors can report deficiencies or violation to the inspectors general of U.S. intelligence agencies and, as permitted by law, to the Senate and House intelligence committees.[33]

iv. Increased Disclosure Requirements

FARA introduced a number of new disclosure requirements for intelligence agencies. First, FARA requires future ODNI Statistical Transparency Reports agencies to separately state the number of U.S. persons and non-US persons that were targets of electronic surveillance.[34] Second, FARA formally mandates that agencies' Section 702 minimization procedures be published.[35] Third, FARA requires the Attorney General to provide new reporting to Congress on the number of surveillance applications and emergency authorizations,[36] and to make each report publicly available and unclassified "to the extent consistent with national security."[37]

v. Requirements for Resuming Abouts Collections

Abouts collection was an aspect of the NSA's Upstream program. As discussed more fully in Section 2(d) below, following significant interaction with the FISC on the lawfulness of Abouts communication, the NSA voluntarily discontinued Abouts collections in March 2017. FARA now ensures that both the FISC and Congress must be informed before Abouts collection can be revived. If the NSA wishes to resume "intentional acquisition of [A]bouts communication," several requirements must be met.[38] First, FISC must issue a certification approving the program and

---

[26] *Id.* § 109 (2018).

[27] Nat'l Sec. Agency, *Querying Procedures Used by the National Security Agency in Connection with Acquisitions of Foreign Intelligence Information Pursuant to Section 702 of the Foreign Intelligence Surveillance Act of 1978, As Amended,* 3 (Sept. 16, 2019), available at: *https://www.intelligence.gov/assets/documents/702%20Documents/declassified/2019_702_Cert_NSA_Querying_17Sep19_OCR.pdf.*

[28] FARA § 106.

[29] Office of the Dir. of Nat'l Intelligence,, *The FISA Amendments Reauthorization Act of 2017: Enhanced Privacy Safeguards for Personal Data Transfers Under Privacy Shield,* 3 (Oct. 15, 2018) available at: *https://www.dni.gov/files/documents/icotr/Summary-FISA-Reauthorization-of-2017—10.15.18.pdf* [*hereinafter* "DNI FARA Summary"].

[30] FARA § 110.

[31] DNI FARA Summary, *supra* note 29.

[32] *See id.*

[33] *See* SWIRE, *supra* note 2 at 3–28—3–29.

[34] FARA § 102(b).

[35] *Id.* § 104 (2018). Although agencies' minimization procedures have already been declassified and published for each year in which the corresponding Section 702 reauthorization was published, this change may result in minimization procedures being published even when the underlying reauthorization is not.

[36] *Id.* § 107.

[37] *Id.*

[38] *Id.* § 103.

"a summary of the protections in place to detect any material breach."[39] Second, the NSA must notify Congress in writing 30 days before resuming Abouts collection, and cannot begin Abouts collection within that thirty-day window.[40] The FISC's order approving the recommencement of Abouts collection must be attached to the notice provided to Congress.[41] Third, if Abouts collection resumes after having satisfied the prior two requirements, the NSA must report all material breaches to Congress.[42] Finally, any FISC opinion certifying the recommencement of Section 702 Abouts collection will be designated as a "novel or significant interpretation of the law," thus requiring appointment of an amicus curiae during authorization proceedings, as well as public release of the opinion.[43] The presence of these requirements within the amended Section 702 adds another level of oversight to the NSA's collection of Section 702 data.

b. FISC Continued to Evaluate 702 Compliance During Annual Reauthorizations

As stated above, FISC must annually review and reauthorize Section 702 programs. Since my prior testimony, FISC has reauthorized Section 702 programs on at least three occasions: in April 2017,[44] October 2018,[45] and December 2019.[46] For each of these reauthorizations, the U.S. government declassified and published (a) the FISC order evaluating and reauthorizing Section 702 programs; and (b) the targeting, minimization, and (starting in 2018) querying procedures approved by the FISC to govern the conduct of Section 702 surveillance.[47] For the 2016 reauthorization, the government also declassified the ODNI/Attorney General certification and the NSA Director's affidavit submitted to FISC.[48]

The FISC reauthorization opinions show the FISC conducting the careful and detailed oversight over Section 702 surveillance I discussed in my 2016 Testimony.[49] FISC continued to examine how Section 702 programs "have been and will be implemented" in practice.[50] It also crafted new requirements for compliance with Section 702. As brief examples of FISC's review:

- The 2016 reauthorization opinion is 99 pages long.[51] The FISC evaluated the NSA's reports of compliance incidents relating to Abouts collection, and the NSA's decision to terminate Abouts collection in response (discussed immediately below). Further, the FISC evaluated the NCTC receiving access to Section 702 information, NSA data deletion questions, and potential issues relating to NSA's Upstream program that had occurred in the past year. The FISC also evaluated the NSA's use of automated tools for tasking decisions; determined

---

[39] *Id.* § 103(b)(3).
[40] *Id.* § 103(b)(2).
[41] *Id.* § 103(b)(3).
[42] *Id.* § 103(b)(5). Material breaches include "significant noncompliance with applicable law or an order of the FISC concerning any acquisition of Abouts communication," *see id.* § 103(b)(1)(B). It can be presumed that other compliance incidents, whether material or not, would be reported to the FISC, as this is the FISC's current requirement for Section 702 programs.
[43] *Id.* § 103(b)(6); *see also* USA FREEDOM Act, Pub. L. 114–23, § 602(a) (2017).
[44] *See generally Mem. Op. & Order [Redacted],* Case Caption [Redacted] (F.I.S.C. Apr. 26, 2017) available at: *https://www.dni.gov/files/documents/icotr/51117/2016_Cert_FISC_Memo_Opin_Order_Apr_2017.pdf* [*hereinafter* "FISC 2016/2017 Reauthorization"].
[45] *See generally Order [Redacted],* Case Caption [Redacted] (F.I.S.C. Oct. 18, 2018) available at: *https://www.intelligence.gov/assets/documents/702%20Documents/declassified/2018_Cert_FISC_Opin_18Oct18.pdf* [*hereinafter* "FISC 2018 Reauthorization"].
[46] *See generally Mem. Op. & Order [Redacted],* Case Caption [Redacted] (F.I.S.C. Dec. 6, 2019) available at: *https://www.intelligence.gov/assets/documents/702%20Documents/declassified/2019_702_Cert_FISC_Opinion_06Dec19_OCR.pdf* [*hereinafter* "FISC 2019 Reauthorization"].
[47] *See generally* FISC 2016/2017 Reauthorization, *supra* note 44; FISC 2018 Reauthorization, *supra* note 45; FISC 2019 Reauthorization, *supra* note 46.
[48] *See generally* FISC 2016/2017 Reauthorization, *supra* note 44.
[49] *See generally* SWIRE, *supra* note 2 at 5–1—5–53.
[50] *Mem. Op. & Order [Redacted],* Case Caption [Redacted], 3 (F.I.S.C. Aug. 26, 2014), available at *https://www.dni.gov/files/documents/0928/FISC%20Memorandum%20Opinion%20and%20Order%2026%20August%202014.pdf; See also* SWIRE, *supra* note 2 at 5–12—5–14.
[51] *See* FISC 2016/2017 Reauthorization, *supra* note 44; Due to extensions granted to review Abouts collection which extended reauthorization proceedings, the 2016 reauthorization appears to have covered Section 702 surveillance in both the years 2016 and 2017. The Attorney General and ODNI filed certifications to reauthorize Section 702 surveillance on September 26, 2016. *See also Government's Ex Parte Submission of Reauthorization Certifications and Related Procedures, Ex Parte Submission of Amended Certifications, and Request for an Order Approving Such Certifications and Amended Certifications [Redacted],* (F.I.S.C. Sept. 26, 2016) available at: *https://www.dni.gov/files/documents/icotr/51117/2016_Certification_Cover_Filing_Sep_26_2016_part_1_and_2_-merged.pdf.* In evaluating Abouts collection issues, FISC granted extensions into March 2017, at which point NSA announced it was terminating Abouts collection. FISC then issued its reauthorization order on April 26, 2017. This reauthorization thus appears to have authorized Section 702 programs for 2016 and 2017.

that reliance on these tools was not sufficient to task a selector; and required the NSA to begin reporting incidents where the NSA did not conduct post-tasking review of acquired communications to determine whether a tasking decision has been proper.

- The 2018 reauthorization opinion is 138 pages long.[52] In its most lengthy discussion, the FISC found FBI querying practices involving U.S. person identities were inconsistent with the Fourth Amendment; this finding was appealed to the FISA Court of Review, which affirmed the FISC,[53] resulting in the FBI modifying its minimization and querying procedures.[54] Additionally, in a novel and significant decision, the FISC held that FARA restrictions on Abouts collection also applied to certain non-Abouts collection. Although the precise collection technique at issue remained redacted, FISC ordered the NSA to report each time it tasked a selector using this technique within 10 days to FISC, presumably to monitor on an ongoing basis that NSA's acquisitions complied with the restrictions of FARA.[55] For this decision, the FISC invited and received amicus briefing.
- The 2019 reauthorization opinion is 83 pages long.[56] It addressed questions about whether the NSA may share information with FBI for targeting purposes, as well as the retention period for Upstream collection after termination of Abouts collection. Additionally, FISC addressed whether 702-acquired information could be captured by intelligence agencies' "user-activity monitoring" (AUM) activities, such as insider threat protection. The FISC preliminarily approved AUM activities, but required all agencies to provide further reporting on the extent of their AUM activities and the amount of 702-acquired information affected by it.

c. NSA Terminated Upstream's Abouts Collection in Connection with FISC's 2017 Section 702 Reauthorization

The NSA's termination of Abouts collection represents a significant development that has occurred since my 2016 Testimony and illustrates the effectiveness of the U.S. system of safeguards for foreign intelligence surveillance. Abouts collection referred to an aspect of the NSA's Section 702 Upstream program. It acquired communications that were not to or from a tasked selector, but which instead mentioned the selector (and were thus described as being "about" that selector). An example would be the NSA receiving an e-mail where the selector e-mail address of the target is included in the body or text of the e-mail, but neither sent nor received that e-mail.[57]

Abouts collection first came to FISC's attention in 2011, when it raised concerns due to acquisition of Multi-Communication Transactions (MCTs).[58] E-mails and similar communications are often not transmitted through the Internet as discrete communications, but instead as part of MCT clusters,[59] what is often called a "thread" of e-mails. This resulted in Upstream acquiring not just communications containing a tasked selector, but also a further cluster of attached communications in which the selector did not appear.[60] For Abouts communication, FISC found this raised heightened privacy concerns, since it resulted in the NSA acquiring communications that did not contain selectors.[61] FISC thus imposed a number of restrictions on Abouts collection, such as requiring the NSA to segregate Abouts collection from other 702-acquired data, to restrict other agencies' access to Upstream collection, to restrict NSA analysts' use of Upstream-collected data, and to purge Up-

---

[52] *See* FISC 2018 Reauthorization, *supra* note 45.

[53] *See In Re: DNI/AG 702(h) Certifications 2018 [Redacted],* Dkt. No. [Redacted] (F.I.S.A. Ct. Rev. July 12, 2019) available at: *https://www.intelligence.gov/assets/documents/702%20Documents/declassified/2018_Cert_FISCR_Opinion_12Jul19.pdf.*

[54] *See Mem. Op. & Order [Redacted],* Case No. [Redacted] (F.I.S.C. Sept. 4, 2019) available at: *https://www.intelligence.gov/assets/documents/702%20Documents/declassified/2018_Cert_FISC_Opinion_04Sep19.pdf*

[55] *See* FISC 2018 Reauthorization, *supra* note 45 at 136–138.

[56] *See* FISC 2019 Reauthorization, *supra* note 46.

[57] Nat'l Sec. Agency, *NSA Stops Certain 702 "Upstream" Activities,* PA–014–18, (Apr. 28, 2017), available at: *https://www.nsa.gov/news-features/press-room/Article/1618699/nsa-stops-certain-section-702-upstream-activities/*.

[58] *See generally* SWIRE, *supra* note 2 at 5–31—5–34.

[59] *See Id.*

[60] *See Id.*

[61] *See Id.*

stream collection on a more expedited basis than other 702-acquired information.[62] These restrictions were memorialized in NSA's Section 702 minimization beginning in 2011.[63]

It appears that in 2016, NSA's Inspector General reviewed NSA's querying of Upstream collections and identified "significant noncompliance" with the FISC's restrictions.[64] This was reported to FISC, which held a hearing and required the government to submit a report on the full extent of querying practices affecting Upstream data as well as a remediation plan.[65] The government provided several rounds of updates to the FISC; however, the FISC on several occasions expressed dissatisfaction with the state of the government's investigation into how querying practices were not complying with existing FISC orders.[66]

Ultimately, on March 30, 2017, the NSA reported to FISC that it would "eliminate 'Abouts' collection altogether."[67] In addition, NSA stated it would "sequester and destroy raw Upstream Internet data previously collected," and "destroy such sequestered Internet transactions as soon as practicable through an accelerated age-off process."[68] Going forward, NSA stated that any communications obtained by Upstream "that are not to or from a person targeted in accordance with NSA's section 702 targeting procedures . . . will be destroyed upon recognition," and that NSA "will report any acquisition of such communications to [FISC] as an incident of noncompliance."[69] The NSA proffered updated minimization procedures to the FISC that memorialized these changes to Upstream.[70]

The FISC accepted the NSA's updated minimization procedures that prohibited Abouts collection.[71] Further, as described above, FARA now requires the NSA to obtain FISC authorization, and provide notification to Congress, prior to recommencing Abouts communication.[72] The NSA also publicly announced its termination of Abouts collection.[73]

The termination of Abouts communication underscores the effectiveness of the U.S. system of safeguards for foreign intelligence. The FISC recognized privacy risks in Abouts collection and imposed heightened requirements on the NSA. Those requirements could not be met, in part due to technical challenges. Internal reviews identified the noncompliance; and it was reported to FISC. FISC insisted on compliance with its privacy restrictions, and the NSA determined this required Abouts collection to end.

d. Statistics on 702 Programs Continue to be Released by the U.S. Government

ODNI publishes annual Statistical Transparency Reports that identify the number of non-U.S. persons who are the targets of tasked selectors under Section 702.[74] My 2016 Testimony referenced that in 2015, there had been 94,368 targets of Section 702 programs.[75] Since then, the Statistical Transparency Reports have provided

---

[62] *See Mem. Op. [Redacted],* Case No. [Redacted] (F.I.S.C. Oct. 3, 2011) available at: *https://www.dni.gov/files/documents/0716/October-2011-Bates-Opinion-and%20Order-20140716.pdf*

[63] *See Mem. Op. [Redacted],* Case No. [Redacted] (F.I.S.C. Nov. 30, 2011) available at: *http://www.fas.org/irp/agency/doj/fisa/fisc1111.pdf*

[64] FISC 2016/2017 Reauthorization, *supra* note 44 at 4.

[65] *See id.*

[66] *See id.* at 4–6.

[67] *Id.* at 6.

[68] *Id.* at 23–24.

[69] *Id.*

[70] *Id.* at 26.

[71] *See id.*

[72] FARA § 103.

[73] Nat'l Sec. Agency, *NSA Stops Certain 702 "Upstream" Activities,* PA–014–18 (Apr. 28, 2017), *available at: https://www.nsa.gov/news-features/press-room/Article/1618699/nsa-stops-certain-section-702-upstream-activities/)*

[74] *See* 50 U.S.C. § 1873(b)(2)(A); SWIRE, *supra* note 2 at 3–36—3–37.

[75] *See* SWIRE, *supra* note 2 at 3–21—3–24.

targeting statistics for subsequent years.[76] The following table provides statistics for targeting of non-US persons under Section 702 since 2016:[77]

Calendar Year	2016	2017	2018	2019
Estimated Number of Section 702 Targets for Non-US Persons	106,469	129,080	164,770	204,968

I add one comment relevant to current discussions about possible changes in U.S. surveillance practices after *Schrems II.* One proposal I have heard would be to end the Section 702 program and have each selector be subject to the one-at-a-time prior approval by a judge under Title I of FISA, the sort of approval that applies to individuals in the U.S. where there is probable cause that they are "agents of a foreign power."[78] There are currently 11 Federal district judges on the FISC; processing over 100,000 individual orders per year would simply not be possible with anything like current staffing with the care and attention to each application that DOJ documents and a judge assesses. As discussed in my 2016 Testimony, Section 702 was created in 2008 as an increase in legal process compared to prior collection done outside of the US.[79] Adding one-at-a-time prior approval by a judge for each selector would thus appear to be a greater change to current practice than some may have realized. That is not a conclusion about what changes the U.S. might contemplate in discussions with the EU, but instead an observation about the nature of the current 702 program.

e. The U.S. Government Continued to Publish Semiannual Assessments of Compliance for 702 Programs

Section 702 requires the AG and ODNI to jointly assess intelligence agencies' compliance with FISA Section 702 and publish their assessment semiannually in a declassified report (the "Semiannual Assessments").[80] The AG (through its National Security Division) and ODNI conduct regular on-site reviews of NSA, FBI, and CIA on at least a bimonthly basis, and they review agencies' targeting and minimization decisions.[81] Using the results of these reviews, the Semiannual Assessments describe types, percentages, and trends of 702 non-compliance issues. The table below summarizes the overall compliance rates, as well as compliance rates for each cat-

---

[76] *See generally* Office of the Dir. of Nat'l Intelligence, *Statistical Transparency Report: Regarding the use of National Security Authorities for Calendar Year 2016* (Apr. 2017) available at: *https://www.dni.gov/files/icotr/ic_transparecy_report_cy2016_5_2_17.pdf; See generally* Office of the Dir. of Nat'l Intelligence, *Statistical Transparency Report: Regarding the use of National Security Authorities for Calendar Year 2017* (Apr. 2018) available at: *https://www.dni.gov/files/documents/icotr/2018-ASTR-CY2017-FINAL-for-Release-5.4.18.pdf; See generally* Office of the Dir. of Nat'l Intelligence, *Statistical Transparency Report: Regarding the use of National Security Authorities for Calendar Year 2018,* (Apr. 2019) available at: *https://www.dni.gov/files/CLPT/documents/2019_ASTR_for_CY2018.pdf; See generally* Office of the Dir. of Nat'l Intelligence, *Statistical Transparency Report: Regarding the use of National Security Authorities for Calendar Year 2019* (Apr. 2020) available at: *https://www.dni.gov/files/CLPT/documents/2020_ASTR_for_CY2019_FINAL.pdf.*

[77] Office of the Dir. of Nat'l Intelligence, *Statistical Transparency Report: Regarding the use of National Security Authorities for Calendar Year 2019,* 14 (Apr. 2020) available at: *https://www.dni.gov/files/CLPT/documents/2020_ASTR_for_CY2019_FINAL.pdf* [*hereinafter* "2019 Statistical Transparency Report"].

[78] 50 U.S.C. § 1801(b).

[79] *See* SWIRE, *supra* note 2 at 3–18—3–19.

[80] 50 U.S.C. § 1881(a)(l)(1).

[81] *See* SWIRE, *supra* note 2 at 5–20—5–23.

[82] Dir. of Nat'l Intelligence & U.S. Att'y Gen., *Semiannual Assessment of Compliance with Procedures and Guidelines Issued Pursuant to Section 702 of the Foreign Intelligence Surveillance Act,* 26–30 (Feb. 2016), available at here: *https://www.dni.gov/files/documents/icotr/14th-Joint-Assessment-Feb2016-FINAL-REDACTED.pdf*

[83] Dir. of Nat'l Intelligence & U.S. Att'y Gen., *Semiannual Assessment of Compliance with Procedures and Guidelines Issued Pursuant to Section 702 of the Foreign Intelligence Surveillance Act,* 27–31 (Nov. 2016), found here: *https://www.dni.gov/files/documents/icotr/15th-702Joint-Assessment-Nov2016-FINAL-REDACTED1517.pdf*

[84] Dir. of Nat'l Intelligence & U.S. Att'y Gen., *Semiannual Assessment of Compliance with Procedures and Guidelines Issued Pursuant to Section 702 of the Foreign Intelligence Surveillance Act,* 27–31 (Aug. 2017), found here: *https://www.dni.gov/files/icotr/16th_Joint_Assessment_Aug_2017_10.16.18.pdf*

[85] Dir. of Nat'l Intelligence & U.S. Att'y Gen., *Semiannual Assessment of Compliance with Procedures and Guidelines Issued Pursuant to Section 702 of the Foreign Intelligence Surveillance Act,* 26–30 (Dec. 2017), found here: *https://www.dni.gov/files/icotr/17th_Joint_Assessment_Dec_2017_10.16.18.pdf*

egory of non-compliance, from December 2014 to November 2017. Note that Semiannual Assessments are published on a lag, meaning that although the statistics below date back to 2014, all of the below statistics have been published since the 2016 period in which my prior Testimony and Privacy Shield were finalized.

Intelligence Agencies Compliance Statistics	Report 14 (Dec. 2014–May 2015)[82]	Report 15 (June 2015–Nov. 2015)[83]	Report 16 (Dec. 2015–May 2016)[84]	Report 17 (June 2016–Nov. 2016)[85]	Report 18 (Dec. 2016–May 2017)[86]	Report 19 (June 2017 to Nov. 2017)[87]
Overall Non-Compliance Rate	0.35%	0.53%	0.45%	0.88%	0.37%	0.42%
Tasking Non-Compliance Rate	42.3%	58.%	50.8%	35.3%	24.9%	28.7%
Detasking Non-Compliance Rate	24.3%	21.5%	13.7%	5.9%	7.5%	7.3%
Notification Non-Compliance Rate	8.7%	5.2%	6.4%	6.8%	11.2%	22.1%
Documentation Non-Compliance Rate	4.9%	2.2%	12.9%	7.5%	14%	23.6%
Minimization Non-Compliance Rate	14.8%	9.9%	14.3%	42.5%	39.1%	17.3%
Miscellaneous/Other Non-Compliance Rate	4.9%	2.5%	2%	1.9%	0.9%	0.7%
Overcollection Non-Compliance Rate	Not reported	Not reported	Not reported	0.1%	Not reported	0.3%

Overall, AG/ODNI concluded in each Semiannual Assessment that "the agencies have continued to implement [targeting and minimization] procedures and follow [applicable] guidelines in a manner that reflects a focused and concerted effort by agency personnel to comply with the requirements of Section 702."[88] Only two incidents of intentional non-compliance were identified in the six Semiannual Assessments that have been published since my 2016 Testimony, each of which was remedied.[89] The Semiannual Assessments enable transparency into the conduct of foreign intelligence surveillance that, to the best of my knowledge, remains unique among leading nations.

f. NSA Declassified its Internal Training Manuals for 702 Programs

Since my 2016 Testimony, NSA has released internal guidance and training documents related to Section 702.[90] The documents show the multi-level training NSA provides to personnel on Section 702 compliance. They include trainings NSA provides to analysts who task selectors to be used in Section 702 surveillance, detailing the process through which NSA analysts must document their rationale for targeting a selector and submit it to an NSA "Adjudicator" for review. The documents also include trainings provided to Adjudicators on reviewing analyst requests to task

[86] Dir. of Nat'l Intelligence & U.S. Att'y Gen., *Semiannual Assessment of Compliance with Procedures and Guidelines Issued Pursuant to Section 702 of the Foreign Intelligence Surveillance Act,* 28–32 (Oct. 2018); found here: *https://www.dni.gov/files/icotr/18th_Joint_Assessment.pdf* [*hereinafter* "Semiannual Report 18"].

[87] Dir. of Nat'l Intelligence & U.S. Att'y Gen., *Semiannual Assessment of Compliance with Procedures and Guidelines Issued Pursuant to Section 702 of the Foreign Intelligence Surveillance Act,* 30–36 (Dec. 2019)., found here: *https://www.intelligence.gov/assets/documents/702%20Documents/declassified/19th%20Joint%20Assessment%20for%20702%20Dec%202019%20-%20Final%20for%20release%20(002)OCR.pdf* [*hereinafter* "Semiannual Report 19"].

[88] This conclusion is from the October 2018 Semiannual Assessment, but is representative of the conclusion of prior Semiannual Assessments. *See, e.g.,* Semiannual Report 18, *supra* note 86 at 48, ("[T]he agencies continued to implement the procedures and follow the guidelines in a manner that reflects a focused and concerted effort by agency personnel to comply with the requirements of Section 702.").

[89] In Semiannual Report 19, there were two issues of intentional non-compliance. The first issue involved FBI running batch queries under proposed, but unapproved, query procedures. These query procedures were eventually approved, but this incident still counted as intentional non-compliance. The second issue involved traditional intentional non-compliance where an FBI analyst queried his name and the name of his co-worker in the FBI database. This analyst was fired, and his security clearance was terminated. *See* Semiannual Report 19, *supra* note 87.

[90] *See* Office of the Dir. of Nat'l Intelligence, *IC on the Record: IC on the Record Guide to Posted Documents,* ICONTHERECORD.TUMBLR.COM, (Oct. 2020), available at: *https://www.intel.gov/ic-on-the-record/guide-to-posted-documents.*

[91] *See* Nat'l Sec. Agency, *Updated FAA 702 Targeting Review Guidance [Redacted],* (May 15, 2017), available at: *https://www.dni.gov/files/icotr/ACLU%2016-CV-8936%20(RMB)%20000911-001000%20-%20Doc%2010.%20NSA%E2%80%99s%20702%20Targeting%20Review%20Guidance.pdf;* NSA's Practical Applications Training. *See also* Nat'l Sec. Agency, *CRSK1304: FAA Section 702 Practical Applications [Redacted]; https://www.dni.gov/files/icotr/ACLU%2016-CV-8936%20(RMB)%20000911-001000%20-%20Doc%2011.%20NSA%E2%80%99s%20702%20Practical%20Applications%20Training.pdf.*

specific selectors, and the checklists used in selector evaluations.[92] Finally, NSA published a comprehensive Section 702 training covering aspects of NSA personnel's compliance duties relating to collecting, processing, analysis, retention, and dissemination of 702-acquired information, as well as obligations to immediately report compliance incidents.[93]

As one comment on possible reforms that may address EU legal concerns, the U.S. government might consider codifying training requirements and other aspects of compliance. Such codification might be done through either statutory or non-statutory means, to address European legal concerns that Section 702 and other safeguards be "required by law."

3. Updates to the Former 215 Program.

In my 2016 Testimony, I discussed "[p]erhaps the most dramatic change in U.S. surveillance law" since the Snowden disclosures: The termination of a bulk telephone record collection program that had been operated under Section 215 of the USA PATRIOT Act, and its replacement with a targeted call records program.[94] This change began when President Obama's Review Group, in which I participated, reviewed the 215 program and found it "not essential to preventing attacks."[95] The USA FREEDOM Act was passed soon thereafter, and prohibited bulk collection under Section 215, as well as under pen register, trap-and-trace, and national security letter authorities. NSA terminated the bulk phone records program on November 29, 2015.[96]

The USA FREEDOM Act thus introduced a targeted telephone call detail records program (the "CDR Program") that operated as I described in my 2016 Testimony.[97] The government had to identify a specific selector that is reasonably suspected of being associated with terrorism (such as a phone number), and obtain a FISC order requiring a communications provider to produce records associated with that selector. The government could only obtain records that were no more than two "hops" from the identified selector.

Since my 2016 Testimony, the NSA voluntarily terminated the CDR Program due to compliance and data-integrity issues it did not believe could be resolved. This section briefly describes the significant events relating to the CDR Program: (a) the NSA's deletion of years' worth of CDRs, followed by its decision to terminate the CDR Program, and (b) the PCLOB's ensuring report on the CDR Program. These NSA actions are another example of the oversight and correction mechanisms built into the U.S. legal system governing foreign intelligence.

a. NSA Voluntarily Deleted 3 Years' Worth of USA FREEDOM Act CDRs, then Discontinued the CDR Program Altogether

The CDR Program was affected by a number of compliance issues that resulted in the NSA deciding to delete years' worth of CDR Program data, then to discontinue the program. Between 2016 and 2019, the NSA provided a number of notices to FISC detailing issues of non-compliance and data-integrity issues.[98] Generally, the non-compliance issues included information omitted from FISA applications, providers transmitting CDRs on expired orders, and training and access incidents involving NSA personnel.[99] The data-integrity issues generally involved the

---

[92] *See* Nat'l Sec. Agency, *FAA702 Adjudicator Training [Redacted],* available at: *https://www.dni.gov/files/icotr/ACLU%2016-CV-8936%20(RMB)%20000911-001000%20-%20Doc%2012.%20NSA%E2%80%99s%20702%20Training%20for%20NSA%20Adjudicators.pdf;* Nat'l Sec. Agency, *FAA 702 Adjudication Checklist [Redacted],* available at: *https://www.dni.gov/files/icotr/ACLU%2016-CV-8936%20(RMB)%20001001-001049%20-%20Doc%2013.%20NSA%E2%80%99s%20702%20Adjudication%20Checklist.pdf*

[93] *See* Nat'l Sec. Agency, *OVSC1203: FISA Amendments Act Section 702 [Redacted],* available at: *https://www.dni.gov/files/icotr/ACLU%2016-CV-8936%20(RMB)%20001001-001049%20-%20Doc%2017.%20NSA%E2%80%99s%20Training%20on%20FISA%20Amendments20Act%20Section%20702.pdf*

[94] SWIRE, *supra* note 2 at 3–16—3–18.

[95] *See id.*

[96] *See* Office of the Dir. of Nat'l Int., *ODNI Announces Transition to a New Telephone Metadata Program,* (Nov. 27, 2015), available at: *https://www.dni.gov/index.php/newsroom/press-releases/press-releases-2015/item/1292-odni-announces-transition-to-new-telephone-meta data-program.*

[97] *See* SWIRE, *supra* note 2 at 3–16—3–18.

[98] *See* Privacy and Civil Liberties Oversight Bd., *Report on the Government's Use of the Call Detail Records Program Under the USA Freedom Act,* 20 (Feb. 2020), available at: *https://documents.pclob.gov/prod/Documents/OversightReport/87c7e900-6162-4274-8f3a-d15e3ab9c2e4/PCLOB%20USA%20Freedom%20Act%20Report%20(Unclassified).pdf* [*hereinafter* "PCLOB CDR Report"].

[99] *See id.* at 21.

NSA receiving erroneous data from certain telecom providers.[100] NSA notified FISC of these incidents, and deleted CDRs associated with these incidents.

In a further incident, when a provider produced inaccurate data, NSA searched for "anomalous data from the other providers," and found data-accuracy issues distributed across providers.[101] Further discussions by the NSA with another provider confirmed it also provided inaccurate data.[102] Ultimately, NSA determined "the providers could not identify for NSA all the affected records, and NSA had no way to independently determine which records contained inaccurate information." [103]

In response, starting on May 23, 2018, the NSA began deleting all CDRs obtained since 2015.[104] As required under FISA, the NSA also notified the PCLOB, Department of Justice (DOJ), and Congressional Oversight committees of its decision.[105] In June 2018, NSA released a statement notifying the public that it had deleted all of its call records under the CDR program due to "technical irregularities in some data received from telecommunications service providers" that had resulted in the NSA having access to some CDRs that NSA was not authorized to receive.[106]

Shortly after, in early 2019, the NSA allowed its last FISC order authorizing CDR collection to expire, thus discontinuing the CDR Program under the USA FREEDOM Act.[107] This decision was based on a balancing of "the program's relative intelligence value, associated costs, and compliance and data-integrity concerns." [108] Accordingly, the number of CDRs collected by the NSA fell from over 434 million in 2018 to approximately 4.2 million in 2019.[109]

b. PCLOB Assessed the USA FREEDOM Act CDR Program

In February 2020, the PCLOB issued a report reviewing the CDR program under the USA Freedom Act (the "CDR Program Report").[110] Since the CDR program had been discontinued by the time the PCLOB's Report was issued, the PCLOB made no recommendations regarding the Act, but did issue five key findings. First, the Board found that the CDR program had been constitutional, and second, that the NSA's collection of two hops of CDR data on an ongoing basis was statutorily authorized.[111] Third, PCLOB found no agency abuse of the CDR Program prior to the NSA's decision to stop CDR collection, and, fourth, no evidence that the NSA received statutorily prohibited categories of information such as name, address, or financial information related to a selector. [112] Finally, the Board found the NSA did not use its authority granted under the USA Freedom Act to attempt to gather certain kinds of metadata (the specifics of which remain redacted).[113] More broadly, the PCLOB agreed with the NSA's decision to stop CDR collection.[114]

---

[100] First, a telecom provider pushed "inaccurate first-hop numbers to the NSA," which the NSA's system could not detect. "Instead, [the system] requested second-hop records using the erroneous first-hop response." Subsequently, the provider fixed the issue and the NSA purged the CDRs containing inaccurate numbers. Second, a telecom provider pushed produced a number of CDRs with inaccurate data to the NSA. The NSA took immediate action to stop receipt of CDRs from the provider. The NSA also found there were four FISA applications that relied on the inaccurate information, which it quickly reported to the FISC. The NSA then deleted associated CDRs and "recalled one disseminated intelligence report generated based on inaccurate CDRs." *Id.* at 22.

[101] *Id.* at 23.

[102] *See id.*

[103] *Id.* at 24.

[104] *See* Nat'l Sec. Agency, *NSA Reports Data Deletion,* Release No: PA–010–18, (June 18, 2018), available at: *https://www.nsa.gov/news-features/press-room/Article/1618691/nsa-reports-data-deletion/*

[105] The DOJ subsequently notified FISC. *See id.*

[106] PCLOB CDR Report, *supra* note 98 at 24.

[107] As a part of the discontinuation, the NSA deleted remaining data collected under the CDR Program, but not data "that had been used in disseminated intelligence reporting or data that was considered 'mission management related information.'" PCLOB CDR Report, *supra* note 98 at 24.

[108] PCLOB CDR Report, *supra* note 98 at 24.

[109] Semiannual Report 19 *supra* note 87 at 32.

[110] *See generally* PCLOB CDR Report, *supra* note 98.

[111] Some of the members of the Board did not join on the constitutional analysis provided in the report. *See id.* at 70–77.

[112] *See* PCLOB CDR Report, *supra* note 98 at 2.

[113] *See id.*

[114] *See* Privacy and Civil Liberties Bd., *Fact Sheet: Report on the NSA's Call Detail Records Program Under the USA Freedom Act,* 2, available at: *https://documents.pclob.gov/prod/Documents/OversightReport/e37f0efb-c85d-4053-b4c1-4159ccbf100f/CDR%20Fact%20sheet%20FINAL.pdf*

In March 2020, Congress reauthorized the USA FREEDOM Act, extending it through December 2023.[115] Thus, there is the possibility that NSA could revive the CDR Program in the future. However, to do so, the NSA would have to obtain FISC orders authorizing the collection of CDRs, and the FISC—as it does in other contexts—could impose safeguards on CDR collection based on the past experience of the now-discontinued CDR Program.

4. Updates to Oversight Safeguards.

My 2016 Testimony describes a comprehensive oversight system for foreign intelligence, including Senate and House intelligence committees, agency Inspectors General, Privacy and Civil Liberties offices in the agencies, and ongoing review by the independent Privacy and Civil Liberties Oversight Board.[116] The structure of these oversight safeguards remains unchanged since 2016. This section briefly discusses updates occurring within the existing oversight framework: (a) PCLOB issuing its PPD–28 report, and (b) activities by Inspectors General.

a. PCLOB Issued its PPD–28 Report

On October 16, 2018, PCLOB published its report on Presidential Policy Directive 28 (PPD-28) (the "PPD–28 Report").[117] To produce the Report, PCLOB reviewed the PPD–28 targeting procedures of the CIA, NSA, and FBI, reviewed ODNI reports on changes to signals intelligence under PPD–28,[118] took comments from the public and NGOs, and held classified briefings and discussions with IC elements. PCLOB found PPD–28 resulted in greater memorialization and/or formalization of privacy protections that had inhered in existing practices.[119] For example, prior to PPD–28, NSA had limited its uses of signals intelligence collected in bulk to the six permissible purposes listed in PPD–28 (such as espionage and threats to U.S. armed forces); PPD–28 resulted in these limitations being memorialized and codified.[120] Additionally, PPD–28 resulted in extending protections previously reserved for U.S. persons to all individuals regardless of nationality. For example, NSA and CIA used PPD–28 procedures to refocus on protecting "personal information of all individuals regardless of nationality."[121] Similarly, NSA, CIA, and FBI minimization procedures now require that "personal information of non-US persons shall only be retained if comparable information of U.S. persons may be retained pursuant to" EO 12333.[122]

Based on its review, PCLOB issued four recommendations for PPD–28's implementation:

1) The National Security Council (NSC) and ODNI should issue criteria for determining which activities or types of data will be subject to PPD–28 requirements;
2) IC elements should consider both the mission and privacy implications of applying PPD–28 to multi-sourced systems;
3) NSC and ODNI should ensure that any IC elements obtaining first-time access to unevaluated signals intelligence update their PPD–28 use, retention and dissemination practices, procedures, and trainings before receiving such data; and

---

[115] *See* USA FREEDOM Reauthorization Act of 2020, H.R. 6172, 116th Congress (May 14, 2020), available at: *https://www.congress.gov/bill/116th-congress/house-bill/6172/text*

[116] *See* SWIRE, *supra* note 2 at 3–26—3–34.

[117] This report was issued on the basis of Section 5 PPD–28, which encouraged PCLOB to provide a report on any matters within PCLOB's mandate, such as the implementation of Executive Branch regulations or policies like PPD-28. *See* Privacy and Civil Liberties Bd., *Report to the President on the Implementation of Presidential Policy Directive 28: Signals Intelligence Activities,* (Oct. 16, 2018), available at: *https://documents.pclob.gov/prod/Documents/OversightReport/16f31ea4-3536-43d6-ba51-b19f99c86589/PPD-28%20Report%20 (for%20FOIA%20Release).pdf* [*hereinafter* "PCLOB PPD–28 Report"].

[118] *See* Office of the Dir. of Nat'l Intelligence, *A Status Report on the Development and Implementation of Procedures Under Presidential Policy Directive 28,* (July 2014), available at: *https://www.dni.gov/files/documents/1017/PPD-28_Status_Report_Oct_2014.pdf; See also* Office of the Dir. of Nat'l Intelligence, *2016 Progress Report on Changes to Signals Intelligence Activities* (Jan. 22, 2016), available at: *https://www.intelligence.gov/index.php/ic-on-the-record-database/results/12-odni-releases-2016-signals-intelligence-reform-progress-report.*

[119] *See generally* PCLOB PPD–28 Report, *supra* note 117.

[120] *See id.* at 6.

[121] *Id.* at 6–7.

[122] *Id.* at 7–8.

4) To the extent consistent with the protection of classified information, IC elements should promptly update their public PPD–28 procedures to reflect any pertinent future changes in practices and policy.[123]

These recommendations were later reviewed by ODNI's Office of Civil Liberties, Privacy, and Transparency (CLPT) in an October 2018 report on the status of implementation of the PCLOB's PPD–28 Report.[124] The CLPT found that the agencies had already implemented all four of these recommendations to the extent possible to maintain national security.[125]

b. Inspectors General

My 2016 Testimony described Federal inspectors general (IGs) as an oversight component that provides a well-staffed and significant safeguard to ensure that Federal agencies comply with internal administrative privacy mandates, including exercising privacy watchdog responsibilities[126]. Since my 2016 Testimony, as is widely known, the Department of Justice Inspector General issued a report on traditional FISA warrants issued in connection with an FBI investigation into a U.S. citizen associated with the Trump campaign;[127] however, this report was not related to Section 702 or surveillance targeting non-US persons. The IG for the ODNI has continued to issue semiannual reports relating to the IC as a whole.[128] The IGs for surveillance agencies have also issued semiannual reports to Congress,[129] and have published on an ongoing basis reports on various investigations relating to intelligence agency activities.[130]

5. Updates to Transparency Safeguards.

My 2016 Testimony discussed how, in the wake of the Snowden disclosures, the U.S. government focused on increasing transparency measures relating to U.S. surveillance, both for companies subject to orders and for government agencies that have requested orders.[131] The transparency safeguards I identified in 2016 have remained in place, and continue to provide valuable information about how foreign intelligence surveillance is conducted by U.S. agencies. This section discusses transparency efforts since 2016: (a) additional releases of Statistical Transparency Reports, (b) continued corporate transparency reporting, (c) the creation of a second, text-searchable IC on the Record database, and (d) continued public release of declassified IC documents.

a. Additional Releases of Statistical Transparency Reports.

As discussed in Section 2(e) above, ODNI produces annual Statistical Transparency Reports that cover the IC's use of multiple types of intelligence.[132] Above, I discussed the numbers of Section 702 targets discussed in Statistical Transparency Reports. I note here that Statistical Transparency Reports go well beyond Section

---

[123] *See id.* at 12–18.

[124] *See* Office of the Dir. of Nat'l Intelligence, *Status of Implementation of PPD–28: Response to the PCLOB's Report,* (Oct. 2018), available at: *https://www.dni.gov/files/icotr/Status of _PPD_28_Implementation_Response_to_PCLOB_Report_10_16_18.pdf* [*hereinafter* "CLPT PPD–28 Implementation Report"].

[125] *See id.*

[126] *See* SWIRE, *supra* note 2 at 3–26—3–28.

[127] *See* Office of the Inspector Gen., *Review of Four FISA Applications and Other Aspects of the FBI's Crossfire Hurricane Investigation,* US Dept. of Justice, (Dec. 2019), available at *https://www.justice.gov/storage/120919-examination.pdf*

[128] *See* Office of the Dir. of Nat'l Intelligence, *ICIG Semiannual Report,* available at: *https://www.dni.gov/index.php/who-we-are/organizations/icig/icig-publications/icig-all-reports*

[129] *See, e.g.,* Office of the Inspector Gen., *Semiannual Report to Congress,* National Security Agency, (Oct. 1, 2019 to Mar. 31, 2020), available at: *https://oig.nsa.gov/Portals/71/Reports/SAR/OCT-MAR%202020%20OIG%20SAR.pdf?ver=2020-09-02-094002-550*

[130] For a sample of reports from the NSA's Office of Inspector General, see, *e.g.,* Office of the Inspector Gen. of the Nat'l Sec. Agency, OFFICE OF INSPECTOR GENERAL: REPORTS, available at: *https://oig.nsa.gov/reports/*.

[131] *See* SWIRE, *supra* note 2 at 3–34—3–38.

[132] *See generally* Office of the Dir. of Nat'l Intelligence, *Statistical Transparency Report: Regarding the use of National Security Authorities for Calendar Year 2016,* (Apr. 2017) available at: *https://www.dni.gov/files/icotr/ic_transparecy_report_cy2016_5_2_17.pdf;* Office of the Dir. of Nat'l Intelligence, *Statistical Transparency Report: Regarding the use of National Security Authorities for Calendar Year 2017,* (Apr. 2018) available at: *https://www.dni.gov/files/documents/icotr/2018-ASTR-CY2017FINAL-for-Release-5.4.18.pdf;* Office of the Dir. of Nat'l Intelligence, *Statistical Transparency Report: Regarding the use of National Security Authorities for Calendar Year 2018,* (Apr. 2019) available at: *https://www.dni.gov/files/CLPT/documents/2019_ASTR_for_CY2018.pdf;* Office of the Dir. of Nat'l Intelligence, *Statistical Transparency Report: Regarding the use of National Security Authorities for Calendar Year 2019,* (Apr. 2020) available at: *https://www.dni.gov/files/CLPT/documents/2020_ASTR_for_CY2019_FINAL.pdf.*

702 and disclose statistics on the number of governmental requests made under other FISA foreign-intelligence authorities, including traditional individual FISA warrant authorities for electronic surveillance or physical searches, pen-register and trap-and-trace authorities, the "business records" authorities used to obtain Call Detail Records, and national security letter authorities. These reports also disclose the number of criminal proceedings in which a notice was provided that the government intended to use or disclose FISA-acquired information. The Statistical Transparency Report is also unique in that it explains the development of U.S. surveillance programs, limitations placed on programs by FISC, and even instances of the NSA discontinuing programs—such as the 2020 Statistical Transparency Report describing the NSA's decision to suspend the CDR Program.[133]

b. Continued Corporate Transparency Reporting

My 2016 Testimony highlighted corporate transparency reporting as an important transparency safeguard that arose shortly after the Snowden disclosures.[134] Five leading U.S. technology companies (Facebook, Google, LinkedIn, Microsoft, and Yahoo!) filed suit with the FISC to gain rights to provide transparency reporting, resulting in a DOJ policy change permitting reporting on ranges of governmental foreign intelligence requests. The USA FREEDOM Act codified the right of companies to issue transparency reports.

Since my 2016 Testimony, corporate transparency reporting has continued as permitted under the USA Freedom Act, with large companies regularly publishing reports on government access requests.[135] As in my 2016 Testimony, this Appendix examines the most recent transparency reports of Facebook and Google—the percentages of users whose records were accessed in the most recent six-month period is smaller than in 2016. In total, the number of customer accounts accessed by the U.S. government for national security in the most recent time period is no more than (1) 118,997[136] for Facebook, out of approximately 2.5 billion[137] active users per month; and (2) approximately 109,497[138] for Google, out of approximately 1.17 billion[139] active users per month. The charts below, similar to the ones provided in my 2016 Testimony, reflect the current data above.

I make the following observation—these percentages are very, very small. Government surveillance requests are far from "pervasive" or "unlimited," as some have suggested.

Facebook	# of Users Accessed in 6 months	Accounts Specified	Percentage based on Users Per Month
Non-Content Requests	0–499	0–499	.0000002%
Content Requests	0–499	117,000–117,499	.000047%
National Security Letters	0–499	500–999	.0000004%

Google	# of Users Accessed in 6 months	Accounts Specified	Percentage based on Users Per Month
Non-Content Requests	0–499	0–499	.0000004%
Content Requests	0–499	107,000–107,499	.00009%
National Security Letters	0–499	1000–1499	.0000012%

[133] *See* 2019 Statistical Transparency Report, *supra* note 77 at 29—30.

[134] *See* SWIRE, *supra* note 2 at 3–37—3–39.

[135] *See id.*

[136] For the time period from July 2019–December 2019, Facebook received the following: 0–499 non-content requests (affecting the same number of accounts); 0–499 content requests (affecting between 117,000 and 117,499 accounts); and 0–499 national security letters (affecting the same number of accounts). *See* FACEBOOK, *United States Law Enforcement Requests for Data,* GOVERNMENT REQUESTS REPORT (2020), *https://govtrequests.facebook.com/country/United%20States/2015-H1.*

[137] *See* STATISTA, *Number of Monthly Active Facebook Users Worldwide as of 4th Quarter 2019* (2020), *https://www.statista.com/statistics/264810/number-of-monthly-active-facebook-users-worldwide/#:~≤text=With%20over%202.7%20billion%20monthly,the%20biggest%20social%20network%20worldwide.*

[138] For the time period from January 2019–June 2019, Google received the following: 0–499 non-content requests (affecting the same number of accounts); 0–499 content requests (affecting between 107,000 and 107,499 accounts); and 500–999 national security letters (affecting between 1000 and 1499 accounts). *See* GOOGLE, *Transparency Report—United States* (2020), *https://transparencyreport.google.com/user-data/us-national-security?hl=en.*

[139] *See* Craig Smith, *365 Google Search Statistics and Much More (2020),* EXPANDED RAMBLINGS.COM (Nov. 30, 2020), *http://expandedramblings.com/index.php/by-the-numbers-a-gigantic-list-of-google-stats-and-facts.*

c. The Government Has Launched New Transparency Websites

In 2013, the ODNI created "IC on the Record," a website on which ODNI posts declassified documents relating to United States foreign intelligence surveillance practices. In doing so, the U.S. government became the first government in the world to maintain a running repository of declassified documents from its foreign intelligence agencies and oversight organs.[140] Since its appearance in 2013 and my 2016 Testimony, IC on the Record has accumulated a substantial amount of NSA internal records, FISC opinions, and other documents and records relating to foreign intelligence surveillance. The IC states that it has disclosed hundreds of documents comprising thousands of pages, including "hundreds of documents relating to Section 702."[141]

Further, since 2016, the publicly-available online channels through which the public has access to intelligence-related documents and court decisions has increased. For one, the FISC maintains an online "Public Filings" database containing a substantial number of its declassified opinions and orders, which has added usefulness in being searchable by docket number.[142] Second, ODNI has created "Intel.gov," a new repository on an official IC website that creates the capability to conduct full text searches on all documents posted on IC on the Record.[143] These resources make the transparency offered by the U.S. government significantly more actionable for researchers, civil-rights organizations, and civil society in monitoring how foreign intelligence surveillance is being conducted.

6. Updates to Executive Safeguards

a. Presidential Policy Directive 28 (PPD–28)

My 2016 Testimony discussed Presidential Policy Directive 28 (PPD–28) as a significant new safeguard that creates an extensive system of privacy protection for signals intelligence activities involving non-US persons.[144] Since my prior testimony, PPD–28 has remained unchanged in substance. As discussed above, PPD–28 has resulted in intelligence agencies codifying PPD–28 protections into targeting and minimization procedures governing their conduct of signals intelligence. More significantly, PPD–28 remained in place during the transition between the Obama and Trump administrations.[145] The Biden administration is reportedly expected to continue or increase current protections under PPD–28.[146] This demonstrates significant continuity among U.S. presidential administrations to maintain the United States' commitment to PPD–28 and the protections it offers to non-US persons.

b. Privacy Shield

My 2016 Testimony discussed Privacy Shield as a significant safeguard for the protection of data relating to EU citizens, since it introduced commitments from the U.S. government to provide remedies to EU citizens, to act promptly and effectively to address EU data protection concerns, and to subject compliance to an ongoing review process.[147] After the *Schrems II* judgment, Secretary of Commerce Ross stated that the Department of Commerce would "continue to administer the Privacy Shield program," and that the ECJ decision "does not relieve participating organizations of their Privacy Shield obligations."[148] This indicated the U.S. government continues to require Privacy Shield organizations to apply Privacy Shield protections to data received under the Shield until the data is deleted.

---

[140] *See* SWIRE, *supra* note 2 at 3–36—3–37.

[141] Office of the Dir. of Nat'l Intelligence, *IC on the Record Guide to Posted Documents,* INTEL.GOV, (Oct. 2020), available at: *https://www.intel.gov/ic-on-the-record/guide-to-posted-documents.*

[142] *See* U.S. Foreign Intelligence Surveillance Ct., *Public Filings—US Foreign Intelligence Surveillance Court,* available at: *https://www.fisc.uscourts.gov/public-filings.* [*hereinafter* "FISC Public Filings Website"].

[143] *See* INTEL.GOV, *IC on the Record Database,* available at: *https://www.intel.gov/ic-on-the-record/guide-to-posted-documents* [*hereinafter* "Intel.gov"].

[144] *See* SWIRE, *supra* note 2 at 3–41—3–46.

[145] *See* CLPT PPD–28 Implementation Report, *supra* note 124 at 4.

[146] *See* Kristen Bryan et. al., *Election 2020: Looking Forward to What a Biden Presidency May Mean for Data Privacy and Data Privacy Litigation,* NATIONAL LAW REVIEW, (Nov. 12, 2020), available at: *https://www.natlawreview.com/article/election-2020-looking-forward-to-what-biden-presidency-may-mean-data-privacy-and*

[147] *See* SWIRE, *supra* note 2 at 3–49.

[148] U.S. Dept. of Commerce, *US Secretary of Commerce Wilbur Ross Statement on Schrems II Ruling and the Importance of EU–US Data Flows* (July 16, 2020), available at *https://www.commerce.gov/news/press-releases/2020/07/us-secretary-commerce-wilbur-ross-statement-schrems-ii-ruling-and.*

7. Updates to Foreign Intelligence Surveillance Court (FISC) Testimony.

Chapter 5 of my 2016 Testimony contained an evaluation of the significant number of FISC opinions that had been declassified following the Snowden disclosures, in a number of cases at the FISC's own order. My assessment reached four primary conclusions:

1. The newly declassified FISC materials support the conclusion that the FISC today provides independent and effective oversight over U.S. government surveillance.
2. The FISC monitors compliance with its orders and has enforced with significant sanctions in cases of noncompliance.
3. In recent years, both the FISC on its own initiative and new legislation have greatly increased transparency.
4. The FISC now receives and will continue to benefit from briefing by parties other than the Department of Justice in important cases.

Since my prior testimony, additional FISC opinions have been published, but I am not aware of any reason to alter these conclusions. This section briefly describes updates that have occurred since 2016 and support the above conclusions: (a) FISC decisions continue to be declassified and published; (b) the FISC and FISA Court of Review have issued further decisions in ACLU litigation discussed in my prior Testimony; and (c) FISC transparency statistics continue to show FISC exercising considerable oversight over government surveillance applications.

a. New and Significant FISC Opinions Continue to be Declassified and Published

The transparency in regard to FISC opinions that I discussed in my 2016 Testimony has continued to the present. Opinions have been published under the USA FREEDOM Act's requirement to publish every FISC "decision, order, or opinion" that contains "a significant construction or interpretation of any provision of law" to the greatest practicable extent.[149] Others have been published in connection with litigation pursued by civil-rights organizations.[150] On the whole, a considerable quantity of FISC opinions have been published and can be accessed through IC on the Record,[151] the FISC's own "Public Filings" website,[152] and in text-searchable form on the Intel.gov repository.[153]

b. Updates to ACLU Litigation Discussed in Prior Testimony

My 2016 Testimony discussed litigation brought by the ACLU following the Snowden disclosures in which the ACLU requested that FISC publish its opinions authorizing the bulk telephone records program under Section 215.[154] The FISC found that the ACLU had Article III standing to seek publication of FISC opinions, and ordered the publication of certain Section 215 program authorizations. Since my 2016 Testimony, the FISA Court of Review confirmed that the ACLU and similar public-interest organizations have Article III standing to bring petitions for publication of FISC opinions.[155] However, in a subsequent decision, FISCR held that the FISC does not have subject-matter jurisdiction to hear challenges by public-interest organizations to the withholding of redacted, nonpublic materials in those opinions.[156]

c. FISC Transparency Statistics

My 2016 Testimony assessed a description of the FISC, in the wake of the Snowden disclosures that FISC acted as a "rubber stamp" for government surveil-

---

[149] 50 U.S.C. § 1872.

[150] *See, e.g.,* IC ON THE RECORD, *Release of the FISC Opinion Approving the 2016 Section 702 Certifications and Other Related Documents* (May 11, 2017), available at: *https://icontherecord.tumblr.com/post/160561655023/release-of-the-fisc-opinion-approving-the-2016* (listing "Other FISA Section 702 and Related Documents" produced in response to Freedom of Information Act litigation).

[151] *See* IC ON THE RECORD, available at: *https://icontherecord.tumblr.com/*.

[152] *See* FISC Public Filings Website., *supra* note 142.

[153] *See* Intel.gov, *supra* note 143.

[154] *See* SWIRE, *supra* note 2 at 5–39—5–41.

[155] *See In Re: Certification of Questions of Law to the Foreign Intelligence Surveillance Court of Review,* No. 18–01 (F.I.S.C. Mar. 16, 2018), *https://www.fisc.uscourts.gov/sites/default/files/FISCR%2018-01%20Opinion%20March%2016%202018.pdf.*

[156] *See In Re Op.s & Orders by the FISC Addressing Bulk Collection of Data Under the Foreign Intelligence Surveillance Act,* No. 18–02 (F.I.S.A. Ct. Rev. Mar. 24, 2020), available at: *https://www.fisc.uscourts.gov/sites/default/files/FISCR%2020%2001%20Opinion%20200424.pdf.*

lance requests.[157] The FISC itself had disputed this characterization, stating in a letter to the Senate that "24.4 percent of matters submitted ultimately involved substantive changes to the information provided by the government or to the authorities granted as a result of Court inquiry or action."[158] The USA FREEDOM Act permitted the Administrative Office of U.S. Courts to issue new statistics on FISC practice that—unlike prior DOJ reporting—did not merely state the number of applications that FISC had denied in full, but rather accounted for all applications that FISC procedures significantly modified, denied in part, or denied in full.[159] This reporting enabled a more complete view of the extent to which FISC subjects government surveillance requests to scrutiny resulting in changes or denial. My 2016 Testimony evaluated the first of these new FISC reports and found that "the FISC either rejected or modified just over 17 percent of all surveillance applications it received in the latter half of 2015."[160]

Since 2016, the FISC has continued to publish its statistics on the number of applications and certifications for surveillance it modifies or denies.[161] These reports show the FISC modifying or denying a greater percentage of governmental surveillance requests than it did during my prior review. The following table summarizes the FISC statistics for each year since my 2016 Testimony:

Year	Total Number Applications Modified	Total Number of Applications Denied in Part	Total Number of Applications Denied	Sum of Applications Modified, Denied in Part, and Denied	Total Number of Applications and Certifications	Percentage of Applications Modified or Denied by FISC
2017[162]	391	50	26	**467**	**1,614**	**29%**
2018[163]	261	42	30	**333**	**1,318**	**25%**
2019[164]	234	38	20	**292**	**1,010**	**29%**

8. Updates to Surveillance-Related Standing Cases

My 2016 Testimony briefly discussed the role that Article III standing may play in attempts to challenge surveillance programs before U.S. courts.[165] This section briefly describes the state of select U.S. cases seeking court review of surveillance programs.

a. *Civil Challenges*—The two primary attempts to file a civil challenge to Section 702 programs are both actively appealing dismissals on standing grounds.[166] In each case, the plaintiffs were granted discovery to prove they had standing and proffered either documents or experts as evidence. However, both suits were ultimately dismissed on standing ground because plaintiffs could not show a significant probability, or show evidence the government would authenticate, that the plaintiffs' communications had been affected by 702 programs or their predecessors. My understanding is that both proceedings are currently on appeal to a Federal circuit court.

b. *Challenges in Criminal Cases*—In at least two criminal cases, defendants have asserted challenges to the constitutionality and lawfulness of Section 702 programs when 702-obtained evidence was proffered against them.[167] The challenges have been heard and adjudicated, in each instance with Section 702 pro-

---

[157] SWIRE, *supra* note 2 at 5–9—5–18.

[158] Letter dated July 29, 2013 from Reggie B. Walton, FISC Chief Judge, to Patrick J. Leahy, Chairman of the U.S. Senate Judiciary Committee 2, *http://www.fisc.uscourts.gov/sites/default/files/Correspondence%20Grassley-1.pdf.*

[159] *See* SWIRE, *supra* note 2 at 5–43—5–48.

[160] *Id.* at 5–14—5–17.

[161] *See* U.S. COURTS, *Director's Report on Foreign Intelligence Surveillance Courts' Activities,* available at *https://www.uscourts.gov/statistics-reports/analysis-reports/directors-report-foreign-intelligence-surveillance-courts.*

[162] Admin. Office of U.S. Cts., *Report of the Director of the Administrative Office of the U.S. Courts on Activities of the Foreign Intelligence Surveillance Courts for 2017,* 4, (Apr. 25, 2018), available at *https://www.uscourts.gov/sites/default/files/ao_foreign_int_surveillance_court_annual_report_2017.pdf*

[163] Admin. Office of U.S. Cts., *Report of the Director of the Administrative Office of the U.S. Courts on Activities of the Foreign Intelligence Surveillance Courts for 2018,* 4, (Apr. 25, 2019), available at *https://www.uscourts.gov/ sites/default/files/fisc_annual_ report_2018_0.pdf.*

[164] Admin. Office of U.S. Cts., *Report of the Director of the Administrative Office of the U.S. Courts on Activities of the Foreign Intelligence Surveillance Courts for 2019,* 4, (Apr. 27, 2020), available at *https://www.uscourts.gov/sites/default/files/fisc_annual_report_2019_0.pdf.*

[165] *See* SWIRE, *supra* note 2 at 5–9—5–10.

[166] *See Jewel v. NSA,* No. C 08–04373, 2019 U.S. Dist. LEXIS 217140 (N.D. Cal. 2019); *Wikimedia Found. v. NSA/Central Sec. Serv.,* 427 F. Supp. 3d 582 (D. Md. 2019).

[167] *See U.S. v. Hasbajrami,* 945 F.3d 641 (2d Cir. 2018); *U.S. v. Mohamud,* 843 F.3d 420 (9th Cir. 2016).

grams being found lawful. In each instance, the defendant was a U.S. person whose communications had been incidentally collected via 702 programs. In both cases, the lawfulness of incidentally acquiring communications of U.S. persons via Section 702 programs was affirmed on at the appellate level.[168] In one case, following this appellate finding, the case was remanded to the district court to evaluate whether any querying of databases containing such incidentally-acquired Section 702 information by the government was constitutional.[169]

ANNEX TO SWIRE TESTIMONY: *Acronyms used in this Appendix*

ACLU	American Civil Liberties Union
AG	Attorney General
DNI	U.S. Director of National Intelligence
DOD	U.S. Department of Defense
DOJ	U.S. Department of Justice
DOJ NSD	U.S. Department of Justice, National Security Division EU European Union
FBI	U.S. Federal Bureau of Investigation
FISA	Foreign Intelligence Surveillance Act
FISC	U.S. Foreign Intelligence Surveillance Court
FISCR	U.S. Foreign Intelligence Surveillance Court of Review
FTC	U.S. Federal Trade Commission
IC	U.S. Intelligence Community
IG	Inspector General
ISP	Internet Service Provider
MCT	Multiple Communication Transactions
NSA	U.S. National Security Agency
NSD	National Security Division
NSL	National Security Letters
OCR	U.S. Department of Health and Human Services Office for Civil Rights
ODNI	U.S. Office of the Director of National Intelligence
OIG	U.S. Office of the Inspector General
PCLOB	Privacy and Civil Liberties Oversight Board
PPD	Presidential Policy Directive
SIGINT	Signals Intelligence
US	United States of America
USA FREEDOM	Uniting and Strengthening America by Fulfilling Rights and Ending Eavesdropping, Dragnet-collection and Online Monitoring
USA PATRIOT	Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism

The CHAIRMAN. Well, thank you very much. And yes, indeed, if there was ever a bipartisan committee, it is this Senate committee. So now we turn to Neil Richards. And Professor Richards is appearing remotely. Do we have a good connection? Alright, good, can you hear us?

Mr. RICHARDS. I can. Can you hear me, sir?

The CHAIRMAN. You bet. You are recognized for 5 minutes to summarize your testimony, more or less——

---

[168] *See U.S. v. Hasbajrami,* 945 F.3d 641 (2d Cir. 2018); *U.S. v. Mohamud,* 843 F.3d 420 (9th Cir. 2016).

[169] *See .S. v. Hasbajrami,* 945 F.3d 641 (2d Cir. 2018) (finding that incidental acquisition of U.S. person communications through Section 702 is lawful, but remanding to district court to determine if querying of databases containing 702-acquired information by the government occurred and if so, whether it violated the defendant's constitutional rights).

**STATEMENT OF PROF. NEIL M. RICHARDS,
KOCH DISTINGUISHED PROFESSOR IN LAW; DIRECTOR,
CORDELL INSTITUTE FOR POLICY IN MEDICINE AND LAW,
WASHINGTON UNIVERSITY IN ST. LOUIS**

Mr. RICHARDS. Thank you, Mr. Chairman. Chairman Wicker, Ranking Member—hopefully less, sir. Chairman Wicker, Ranking Member Cantwell and other distinguished members of this committee, thank you for the opportunity to testify at this important hearing. My name is Neil Richards and I am the Koch Distinguished Professor of Law at Washington University in St. Louis where I also co-Direct the Cordele Institute for Policy, Medicine and Law. I am here as an expert on privacy, like my friend Professor Swire. I was also an independent expert witness in *Schrems II,* in my case for the Data Protection Commissioner of Ireland.

The opinions I offer today, however, are my own, and I would like to make three points in my opening remarks. First, the Schrems litigation is a creature of distrust. This distrust comes from the inadequacy of existing Federal privacy safeguards, rights, and remedies, and also, as other panelists have mentioned, from Edward Snowden's 2013 surveillance revelations that led Mr. Schrems to sue in the first place. Two dimensions of the *Schrems II* holding our paramount importance to Congress as it confronts privacy reform.

One is that any successor to the Privacy Shield will require Congress to enact surveillance reform that limits the scope of surveillance and provides meaningful and binding individual remedies to challenge illegality. The other consequence of *Schrems II* is a particular relevance to this committee. U.S. privacy laws are not yet sufficient to meet EU laws cross border requirements of adequacy, which is to say that U.S. privacy laws do not yet offer protections of personal data held by companies that are essentially equivalent to those in the EU.

This matters because adequacy will let EU data flow from Ireland to the U.S. as easily as it can currently flow from Germany to France. Adequacy would make second best mechanisms like the model contractual clause as the Privacy Shield arrangements unnecessary. This leads us to my second main point regarding this committee's bipartisan work on consumer privacy reform, which I believe can solve some of the challenges for data flows and privacy law raised by *Schrems II.*

Comprehensive consumer privacy reform from this committee, coupled with Federal surveillance reform, could result not just in another second best international data transfer agreement, but in an adequacy determination by the European Commission. Under the GDPR, adequacy requires essential equivalence to EU protections, including the rule of law and respect for privacy as a fundamental right in commercial and surveillance contexts. The ECJ in *Schrems II* specified three factors as most important here. First, appropriate safeguards. Second, enforceable rights. And third, effective legal remedies. These principles are necessary for cross-border transfers and for adequacy. They would also, I believe, be a good roadmap for American consumer privacy reform. This committee has already generated draft bills in a good way toward meeting some of these requirements. For example, the draft bill in-

troduced by Senator Cantwell would provide a variety of rights similar to and potentially essentially equivalent to those in the GDPR.

Critically, the Cantwell bill also includes a private right of action for consumers who are injured by unlawful data processing, something that the challenge of *Schrems II* seems to require. I am also a fan of Senator Schatz's Data Care Act, and the approach of Title II of Chairman Wicker's SAFE DATA Act, which has provisions for algorithmic bias detection, data broker registration, filter bubble transparency, and critically abusive trade practices stemming from manipulated interface design. Third, and finally, there is a better way forward than our status quo of distrust.

In a series of published papers, Professor Woodrow Hartzog and I have sought to identify the factors that could get us beyond the dangerous fictions of notice and choice, or even of control-based privacy regulation, and use privacy law to create value for companies as well as protecting consumers. Our trust research indicates that companies who seek trust must be honest, they must be discreet, they must be protective, and they must be loyal. And that where the market provides insufficient incentives, the law can help. In a draft article, we have also articulated a duty of loyalty to privacy law, a duty that actually bears some similarities to Title II of the Wicker bill.

In sum, the Schrems litigation is a creature of distrust. It has created problems for American law and commerce, but it has also created a great opportunity. That opportunity lies before this committee, the chance to regain American leadership in global privacy and data protection by passing a comprehensive law that provides appropriate safeguards, enforceable rights, and effective legal remedies for consumers.

Passing such a law would not just safeguard the ability to share personal data across the Atlantic. If done right, it will build trust between the United States and our European trading partners and between American companies and the European and American customers.

The way forward requires us to recognize that strong, clear, trust building rules aren't hostile to business interests. That we need to preserve effective consumer remedies and State level regulatory innovation. And that we should seriously consider some kind of duty of loyalty.

In that direction, I believe, lies not just consumer protection, but international cooperation and economic prosperity. Thank you.

[The prepared statement of Mr. Richards follows:]

PREPARED STATEMENT OF PROF. NEIL M. RICHARDS, KOCH DISTINGUISHED PROFESSOR IN LAW, DIRECTOR, CORDELL INSTITUTE FOR POLICY IN MEDICINE & LAW, WASHINGTON UNIVERSITY IN ST. LOUIS

Chairman Wicker, Ranking Member Cantwell, and other distinguished Members of this Committee, thank you for the opportunity to testify at this important hearing examining the future of trans-Atlantic data flows and of American privacy law in light of the European Court of Justice's invalidation of the Privacy Shield arrange-

ment in the *Schrems 2* case which.[1] My name is Neil Richards, and I am the Koch Distinguished Professor in Law at Washington University in St. Louis, where I also co-Direct the Cordell Institute for Policy in Medicine and Law. I am here as an expert in privacy law, which I have studied, taught, written about, and practiced for the past two decades. I was also asked by the Data Protection Commissioner of Ireland to serve as one of her independent experts in U.S. law in *Schrems 2,* alongside Mr. Andrew Serwin, a distinguished privacy lawyer now with the firm of DLA Piper. The opinions I offer today are my own. They are not necessarily those of either the Irish Data Protection Commissioner or Washington University in St. Louis.

As someone who has followed technology and privacy policy closely since the 1990s, I am deeply encouraged that Congress—and particularly this Committee under Senator Wicker's and Senator Cantwell's leadership—is taking seriously the urgent need for comprehensive, reasonable, but consumer protective information privacy legislation. This is something that in my opinion is long overdue—Congress came close to passing such a law in 1974, but failed to reach an agreement on private sector data because of concerns about its effect on industry.[2] As we know all too well, this is a pattern that has repeated itself all too often over the past fifty years. It is my fervent hope that this time will be different, and that Congress will not just pass a comprehensive privacy bill, but one that gets it right, that provides clear but substantive rules for companies, and which provides adequate protections and effective remedies for consumers. A law that meets these features will not just protect consumers—it will be good for business as well, by helping enable transatlantic data flows and building the consumer trust that is essential for long-term sustainable economic prosperity for all.

In awareness of the limited time I have for these opening remarks, I would like to offer three observations. First, I will explain what I understand the judgment in *Schrems 2* to require, with particular emphasis on factors within the jurisdiction of this Committee. Second, I will illustrate some ways in which this Committee's work can solve some of the challenges for data flows and privacy law that the *Schrems 2* judgment raises or illustrates. Third, I will argue that this Committee should pass a strong privacy law that builds the consumer trust that is so essential to sustainable and profitable commerce.

I. The *Schrems 2* Case

Privacy is a human right recognized around the world and here in the United States. Protections for privacy run throughout our Constitution, and the "reasonable expectation of privacy" test is at the core of our Fourth Amendment protections against unreasonable searches and seizures.[3] As the Supreme Court recognized in the *Carpenter* decision two years ago, these constitutional privacy protections extend to significant categories of human information that are held on our behalf by private companies.[4] In 1974, when it passed the Privacy Act, Congress recognized that "privacy is a personal and fundamental right."[5] Nevertheless, to date, both Congress and the state legislatures have insufficiently protected information privacy against private actors, particularly in the digital context.

Under European law, both privacy and data protection are fundamental rights expressly protected by the European Charter of Fundamental Rights and Freedoms.[6] In the European Union (EU), the government is required to protect fundamental rights (including privacy rights) against both public and private actors. Consequently, privacy and data protection are specifically protected in the EU by its General Data Protection Regulation or "GDPR."[7] As relevant to this hearing, the GDPR does two things. First, it regularizes and limits the collection and processing of personal data by private actors, including companies.[8] Second, it places limitations on the ability of EU personal data to leave the EU, such as when U.S. tech

---

[1] C–311/18, Data Protection Commissioner v. Facebook Ireland Ltd., *http://curia.europa.eu/juris/document/document.jsf?docid= 228677&mode=req&pageIndex=1&dir=&occ=rst&part=1&text=&doclang=EN&cid=10716034.* (hereinafter "*Schrems 2*").

[2] E.g., SARAH E. IGO, THE KNOWN CITIZEN: A HISTORY OF PRIVACY IN MODERN AMERICAN 257–61 (2018); LAWRENCE CAPPELLO, NONE OF YOUR DAMN BUSINESS: PRIVACY IN THE UNITED STATES FROM THE GILDED AGE TO THE DIGITAL AGE 200–03 (2019).

[3] E.g., *Griswold v. Connecticut,* 381 U.S. 479 (1965); *Katz v. United States,* 389 U.S. 347 (1967); *Riley v. California,* 573 U.S. 373 (2014).

[4] Carpenter v. United States, 585 U.S. ___; 138 S. Ct. 2206 (2018).

[5] Privacy Act of 1974, § 2(a)(4), P.L. 95–579.

[6] Charter of Fundamental Rights of the European Union: 2010 O.J. (C83) 389. Proclaimed by the Commission, 7 December 2000. Proclamation and text at 2000 O.J. (C364) 1.

[7] See Commission Regulation 2016/679, 2016 O.J. (L 119) 1 (EU) (providing the new GDPR).

[8] Chris Jay Hoofnagle, Bart van der Sloot & Frederik Zuiderveen Borgesius, *The European Union general data protection regulation: what it is and what it means,* 28:1 Info. & Comms. Tech. L. 65 (2019).

companies use EU data to fulfill search or GPS requests, store it in the cloud, or use it for HR purposes.[9] In an ideal case, the GDPR allows the personal data of Europeans to flow to a country whose privacy law has been deemed "adequate."[10] But American privacy law has never been deemed "adequate," in large part because America lacks a comprehensive, protective privacy law that allows people to enforce their privacy rights against companies as well as the government.[11] As a result, the legality of the trans-Atlantic data trade has been based upon a set of mechanisms that are second-best—including the model contracts and international executive agreements like the Safe Harbor and Privacy Shield at issue in the *Schrems* litigation.

The *Schrems* litigation is a creature of the costly distrust produced by inadequate Federal privacy laws, protections, and remedies against both government and corporate surveillance. The first *Schrems* decision of 2015 invalidated the Safe Harbor Agreement based upon the revelations about U.S. Surveillance practices by Edward Snowden.[12] This was replaced by the Privacy Shield Agreement, the legality of which was a key issue in the *Schrems 2* litigation. This past July, the European Court of Justice ruled in *Schrems 2,* striking down the Privacy Shield and casting doubt on the mechanism of the standard contractual clauses as a means of transfer to the US.[13] Because the United States has not been deemed to have an "adequate" level of privacy protections, EU Data Protection regulators are now able to suspend transfers of EU personal data to the United States. Indeed, the Irish Data Protection Commissioner has already initiated such proceedings against Facebook, the American company at issue in the *Schrems* litigation.[14]

Two dimensions of the Schrems 2 holding are of paramount importance to Congress as it confronts privacy reform. The first is that any successor to the Privacy Shield would seem to require Congress to enact surveillance reform. The European Courts are particularly concerned that EU citizens whose data is exported to the United States lack meaningful remedies to challenge the legality of the ways that their data may be processed, and the ways in which it may be accessed (particularly in bulk) by the U.S. Intelligence Community.[15] In particular, the European Court of Justice found in *Schrems 2* that the principal defect of the Privacy Shield mechanism was that it failed to offer a binding legal remedy for violations of EU fundamental data protection rights. The Privacy Shield did not allow EU citizens to sue the U.S. government for violations of their rights, but it did create an "Ombudsperson" mechanism within the U.S. State Department, who could act as a kind of complaints desk and investigator. As the European Court of Justice put it, however, "there is nothing [ ] to indicate that [the Privacy Shield] ombudsperson has the power to adopt decisions that are binding on those intelligence services and does not mention any legal safeguards that would accompany that political commitment on which data subjects could rely. . . . Therefore, the ombudsperson mechanism to which the Privacy Shield Decision refers does not provide any cause of action before a body which offers the persons whose data is transferred to the United States guarantees essentially equivalent to those required by Article 47 of the Charter."[16]

The second dimension of the *Schrems 2* decision of relevance to Congress—and of particular relevance to this Committee—is that U.S. privacy laws are not yet "adequate," which is to say that they do not yet offer protections for personal data held by companies that are "essentially equivalent" to those in the EU. This matters because "adequacy" would let the U.S. be treated essentially as a part of Europe for purposes of EU data flow restrictions. If the U.S. were to be deemed to have an "adequate" level of data protection, then "second-best" mechanisms like the model contractual clauses and Privacy Shield arrangements would become unnecessary. While I understand the kinds of surveillance reforms necessitated by the first dimension of the *Schrems 2* judgment to be more appropriately part of the Senate Judiciary Committee's and Senate Intelligence Committee's jurisdictions, the consumer

---

[9] See Paul M. Schwartz & Karl-Niklaus Peifer, *Transatlantic Data Privacy,* 106 GEO. L. J. 115, 130–31 (2017).

[10] GDPR Art. 45.

[11] Paul M. Schwartz & Karl-Niklaus Peifer, *Transatlantic Data Privacy,* 106 GEO. L. J. 115, 158–61 (2017).

[12] 3 Case C–362/14, Schrems v. Data Prot. Comm'r, 2015 E.C.R. 650,191 (Oct. 6, 2015).

[13] *See Schrems 2* at pp. 61–62.

[14] See Shane Phelan & Adrian Weckler, *Facebook in legal battle over order from regulator to halt data transfer to United States,* THE IRISH INDEPENDENT, Sept. 12, 2020, *https://www.independent.ie/business/technology/facebook-in-legal-battle-over-order-from-regulator-to-halt-data-transfer-to-united-states-39524581.html.*

[15] *Schrems 2,* ¶¶ 65, 187, 194.

[16] *Schrems 2* ¶¶ 196–97.

privacy reforms suggested by the second dimension of the judgment are not merely part of this Committee's jurisdiction, but would seem to me to fall squarely within the bipartisan comprehensive consumer privacy reform project that the Committee has already embarked upon. It is to that issue that I will now turn.

II. Surveillance and Consumer Privacy Reform After *Schrems 2*

As Congress considers comprehensive consumer privacy reform, that reform effort will inevitably intersect with the cross-border data transfer issue raised by the *Schrems* litigation and the invalidation of both the Safe Harbor and Privacy Shield arrangements. To solve the problem of trans-Atlantic data transfers and the GDPR, there are essentially three options. First, the United States could do nothing. This would devastate the lucrative and commerce-enhancing trans-Atlantic data trade and result in so-called "data localization," which would require U.S. companies to build expensive data centers in Europe, and process EU citizens' data there at a significant competitive disadvantage to their international competitors. The second option would be for the Executive Branch to negotiate a third, more-protective version of Safe Harbor/Privacy Shield, which would undoubtedly result in uncertainty as an inevitable *"Schrems 3"* challenge rumbled slowly through the Irish and European Courts once again. While it is impossible to perfectly anticipate the results of such a lawsuit, I can say with confidence that without substantial surveillance and consumer privacy reform, the litigation would be likely to end up being invalidated on similar grounds to the Safe Harbor Agreement struck down in *Schrems 1* and the Privacy Shield Agreement struck down in *Schrems 2*.

But there is a third way. Comprehensive consumer privacy reform from this Committee, coupled with Federal surveillance reform could result not just in another second-best international data transfer agreement, but in an adequacy determination by the European Commission. In fact, the *Schrems 2* judgment points the way towards such an outcome. As the European Court of Justice explained in that case, Article 45(1) of the GDPR permits the European Commission to determine that the U.S. could have an "adequate level of protection." The European Court of Justice explains further that "the term 'adequate level of protection' must, as confirmed by recital 104 of [the GDPR], be understood as requiring the third country in fact to ensure, by reason of its domestic law or its international commitments, a level of protection of fundamental rights and freedoms that is essentially equivalent to that guaranteed within the European Union by virtue of the regulation, read in the light of the Charter."[17] Article 45 of the GDPR explains this requirement in further detail by explaining that adequacy requires an inquiry into

> *(a)* the rule of law, respect for human rights and fundamental freedoms, relevant legislation, both general and sectoral, including concerning public security, defence, national security and criminal law and the access of public authorities to personal data, as well as the implementation of such legislation, data protection rules, professional rules and security measures, including rules for the onward transfer of personal data to another third country or international organisation which are complied with in that country or international organisation, case-law, as well as effective and enforceable data subject rights and effective administrative and judicial redress for the data subjects whose personal data are being transferred;
>
> *(b)* the existence and effective functioning of one or more independent supervisory authorities in the third country or to which an international organisation is subject, with responsibility for ensuring and enforcing compliance with the data protection rules, including adequate enforcement powers, for assisting and advising the data subjects in exercising their rights and for cooperation with the supervisory authorities of the Member States; and
>
> *(c)* the international commitments the third country or international organisation concerned has entered into, or other obligations arising from legally binding conventions or instruments as well as from its participation in multilateral or regional systems, in particular in relation to the protection of personal data.[18]

It is a tremendous (and to my mind disappointing) irony that, even though the Privacy Shield was struck down as insufficient, the privacy protections against commercial processing offered to EU citizens whose data was protected by Privacy Shield was substantially greater than that extended to American citizens under U.S. law.

---

[17] *Schrems 2* ¶94 (citing GDPR Art. 45, GDPR Recital 104).
[18] GDPR Art. 45(2).

Yet even if the United States does not seek or achieve an adequacy determination from the European Commission, the level of privacy protection given to personal data in the United States is still relevant to the sustainability of both the model contract mechanism for data transfers and any future, hypothetical "Privacy Shield 2." This is because, as the *Schrems 2* judgment explains, transfers under the second-best option of model contracts or Privacy Shield-type agreements will still require an inquiry into something very much like the adequacy of data protection rights available in the United States.[19] The European Court of Justice specified these requirements clearly as being (1) appropriate safeguards, (2) enforceable rights, and (3) effective legal remedies.[20] A few additional observations about what these requirements would mean in practice is warranted, because I think they offer not just a guide to compliance with the GDPR, but also a good road map for U.S. privacy reform. As I understand these concepts, "appropriate safeguards" means that personal information will be processed in ways that are lawful, appropriate, accurate, secure, and not in ways that harm, expose, mislead, misinform, or manipulate American consumers.[21] "Enforceable rights" means that consumers can make claims against companies regarding how their data is collected, used, and disclosed, whether we are talking about rights of access and correction, rights to prevent the sale or transfer of data for purposes unrelated to the reasons the data was collected in the first place, the placement of duties of care, loyalty, and confidentiality on companies, or independent oversight of commercial uses of data by the FTC or a new independent data protection agency. Finally, "effective legal remedies" means that where consumers have legal rights, they can actually vindicate those rights in court, which means private rights of action (whether for damages or injunctive relief) that are not bogged down by excessive administrative exhaustion requirements, corporate *mens rea* requirements, broad statutory defenses and safe harbors, or the difficulties of navigating standing doctrine.

This Committee has already generated draft bills that go a good way towards meeting some of these requirements. For example, Senate Bill 2968, The Consumer Online Privacy Rights Act introduced by Sen. Cantwell, would provide a variety of rights similar (and potentially "essentially equivalent") to those in the GDPR, like rights of access, deletion, and correction, data minimization, data security requirements to avoid harming consumers, and algorithmic impact assessments.[22] The bill would also provide a private right of action for consumers injured by unlawful data processing, something that the challenge of *Schrems 2* seems to require.[23] Senate Bill 2961, The Data Care Act introduced by Sen. Schatz, is a bold and farsighted statute that would place duties of care, confidentiality and loyalty on companies that collect personal data as part of interstate commerce, along with an expansion of FTC and state enforcement authority.[24] I am also a fan of some of the provisions of Title II of Senate Bill 4626, The Safe Data Act introduced by Chairman Wicker, which has provisions for algorithmic bias detection, data broker registration, filter bubble transparency, and, critically, abusive trade practices stemming from manipulative interface design.[25]

These three factors—appropriate safeguards, enforceable rights, and effective legal remedies—are helpful guidelines as this Committee goes about its work. They will be important regardless of whether this Committee seeks an adequacy determination from the European Commission to permit American companies to participate in the trans-Atlantic data trade, whether this Committee wants to avoid another *Schrems 1* or *Schrems 2,* whether this Committee wants to give American con-

---

[19] *Schrems 2* ¶ 104 ("The assessment required for that purpose in the context of such a transfer must, in particular, take into consideration both the contractual clauses agreed between the controller or processor established in the European Union and the recipient of the transfer established in the third country concerned and, as regards any access by the public authorities of that third country to the personal data transferred, the relevant aspects of the legal system of that third country. As regards the latter, the factors to be taken into consideration in the context of Article 46 of that regulation correspond to those set out, in a non-exhaustive manner, in Article 45(2) of that regulation."); GDPR Art. 46(1) ("In the absence of [an adequacy] a decision pursuant to Article 45(3), a controller or processor may transfer personal data to a third country or an international organisation only if the controller or processor has provided appropriate safeguards, and on condition that enforceable data subject rights and effective legal remedies for data subjects are available.").

[20] *Schrems 2* ¶ 103.

[21] See Woodrow Hartzog & Neil Richards, *Privacy's Constitutional Moment and the Limits of Data Protection,* 61 B.C. L. REV. 1687 (2020) (suggesting a range of safeguards for American privacy law).

[22] S. 2968, 116th Cong. 1st Sess. (Dec. 3, 2019).

[23] See id. tit. III.

[24] S. 2961, 116th Cong. 1st Sess (Dec. 2, 2019).

[25] S. 4626, 116th Cong. 2d Sess. (Sept. 17, 2020).

sumers equivalent protection under American law to that which EU consumers received under the Privacy Shield, or whether this Committee merely wants to pass a meaningful consumer privacy protection bill that protects American consumers and provides clear but meaningful protective guard rails for companies to stay within as part of the digital economy.

With respect to this process going forward, however, let me be clear about three essential features that I believe consumer privacy reform in the United States must recognize. First, the model of "notice and choice" under which the United States has regulated privacy for the past twenty-five years has been an unmitigated disaster. Constructive "notice" through privacy policies and fictitious "choice" through limited opt-outs have created both an illusion of consumer control and enabled largely unrestricted data aggregation.[26] Our law has not given consumers control; it has instead left them largely defenseless and able to be tracked, sorted, harmed, discriminated against, marketed to, ideologically polarized, and manipulated by private companies. Any meaningful privacy reform that is "consumer protective" in anything more than name, must place substantive limits on the ability of companies to collect, use, and sell personal data without meaningful constraint.[27]

Second, as the European Court of Justice recognized, private rights of action are an essential tool for vindicating legal rights. America's next-generation privacy law should not authorize "gotcha" private claims, or massively aggregated class action suits that risk ruinous liability for technical violations. But it should provide what the European Court of Justice calls both enforceable rights and effective legal remedies, even if such remedies offer in some cases "merely" effective injunctive relief to prevent violations.

Third, and finally, I have concerns about bills that are broadly pre-emptive of state causes of action. State legislatures and state attorneys general have often valiantly protected consumer privacy rights in the digital age in the absence of a general Federal privacy law.[28] They have invented new and needed legal protections like data breach notification laws, which have spread throughout the country and around the world.[29] The great American jurist Louis Brandeis famously referred to

---

[26] See, *e.g.,* Neil Richards & Woodrow Hartzog, Taking Trust Seriously in Privacy Law 19 STAN. TECH. L. REV. 431 (2016); Neil Richards & Woodrow Hartzog, The Pathologies of Digital Consent, 96 WASH. U. L. REV. 1461, 1463 (2019); Woodrow Hartzog & Neil Richards, *Privacy's Constitutional Moment and the Limits of Data Protection,* 61 B.C. L. REV. 1687 (2020).

[27] See, *e.g.,* Neil Richards & Woodrow Hartzog, Taking Trust Seriously in Privacy Law 19 STAN. TECH. L. REV. 431 (2016); Neil Richards & Woodrow Hartzog, The Pathologies of Digital Consent, 96 WASH. U. L. REV. 1461, 1463 (2019); Woodrow Hartzog & Neil Richards, *Privacy's Constitutional Moment and the Limits of Data Protection,* 61 B.C. L. REV. 1687 (2020).

[28] See Danielle K. Citron, *The Privacy Policymaking of State Attorneys General,* 92 NOTRE DAME L. REV. 747 (2017).

[29] California passed the first data breach notification law in 2012. See CAL. CIV. CODE §§ 1798.29, .82, .84 (2012). Today, not only do state data breach laws apply across the United States, but Federal laws like the Gramm-Leach-Bliley Act (GLBA), the Health Insurance Portability and Accountability Act (HIPAA), and the Sarbanes-Oxley Act also contain notification requirements, and even the GDPR has incorporated this American legal invention into its comprehensive regulatory scheme. See 16 C.F.R. § 682.3(a); 45 C.F.R. §§ 164.308-.314; 16 C.F.R. §§ 314.3–314.4; ALASKA STAT. § 45.48.010 et seq. (2007); ARIZ. REV. STAT. § 44–7501 (2013); ARK. CODE § 4–110-101 et seq. (2004); CAL CIV. CODE §§ 1798.29, .82, .84 (2012); COLO. REV. STAT. § 6–1–716 (2002); CONN. GEN. STAT. § 36a-701b (2011); DEL. CODE Tit. 6, § 12b-101 et seq. (2011); FLA. STAT. §§ 501.171, 282.0041, 282.318(2)(I) (2010); GA. CODE §§ 10–1–910, -911, -912 § 46–5–214 (West); HAW. REV. STAT. § 487n-1 et seq.(2008); IDAHO STAT. §§ 28–51–104 To -107 (2008) ; 815 ILL. COMP. STAT. ANN. §§ 530/1 to 530/25 (2008); IND. CODE §§ 4–1–11 et seq., 24–4.9 et seq.(2014); IOWA CODE §§ 715c.1, 715c.2 (2015); KAN. STAT. § 50–7a01 et. seq. (2008); KY. REV. STAT. ANN. §§ 365.732, 61.931 To 61.934 (West); LA. REV. STAT §§ 51:3071 et seq. 40:1300.111 To .116 (West); ME. REV. STAT. tit. 10 § 1347 et seq. (2009); MD. CODE COM. LAW §§ 14–3501 et seq. (2013), MD. STATE GOVT. CODE §§ 10–1301 To -1308 (2007); MASS. GEN. L. § 93h-1 et seq. (2006); MICH. COMP. LAW §§ 445.63,445.72 (2014); MINN. STAT. §§ 325e.61, 325e.64 (2011); MISS. CODE § 75–24–29 (2014); MO. REV. STAT. § 407.1500 (2014); MONT. CODE §§ 2–6–504, 30–14–1701 et seq. (2014); NEB. REV. STAT. §§ 87–801, -802, -803, -804, -805, -806,—807 (2014); NEV. REV. STAT. §§ 603.A.010 et seq., 242.183 (2013); N.H. REV. STAT. §§ 359–C:19, -C:20,—C:21 (2009); N.J. STAT. ANN. § 56:8–163 (2012); N.Y. GEN. BUS. L. § 899-Aa, N.Y. STATE TECH. L. 208 (McKinney 2014); N.C. GEN. STAT. §§ 75–61, 75–65 (2012); N.D. CENT. CODE § 51–30–01 et seq (2008).; OHIO REV. CODE §§ 1347.12, 1349.19, 1349.191, 1349.192 (2004); OKLA. STAT. §§ 74–3113.1, 24–161 to -166 (2014); OR. REV. STAT. § 646a.600 to .628 (2011); 73 PA. STAT. § 2301 et seq. (2013); R.I. GEN. LAWS § 11–49.2–1 et seq. (West); S.C. CODE § 39–1–90 (West); TENN. CODE § 47–18–2107 (2014); TEX. BUS. & COM. CODE §§ 521.002, 521.053 (2014), TEX. ED. CODE § 37.007(B)(5) (2013); UTAH CODE §§ 13–44–101 et seq. (2010); Vt. Stat. Tit. 9 § 2430, 2435 (2007); Va. Code § 18.2–186.6, § 32.1–127.1:05 (2012); WASH. REV. CODE § 19.255.010, 42.56.590 (2013); W.V. CODE §§ 46a-2a-101 et seq. (West); WIS. STAT. § 134.98 (2009); WYO. STAT. § 40–12–501 et. seq. (2007); D.C. CODE § 28–3851 et seq. (2013); 10 LAWS OF PUERTO RICO § 4051 et seq.; V.I. CODE TIT. 14, § 2208.

state regulatory experimentation as our "laboratories of democracy,"[30] and in this time of uncertainty and rapid technological change, we should be reluctant to deprive ourselves of this opportunity for regulatory innovation. Moreover, where state private causes of action like negligence or the privacy torts are sometimes the only form of relief available to plaintiffs, I believe that it would be unwise for a Federal law to pre-empt state causes of action, at least without providing equivalent Federal protections.

III. Strong Privacy Safeguards Build Consumer Trust

The *Schrems 2* litigation has certainly created problems for American privacy law, but it has also created a pathway towards the resolution of those problems, whether through an adequacy determination, comprehensive privacy and surveillance reform, or both. In the time that I have left, however, I would like to make one final point, which is that as this Committee considers privacy reform it give serious consideration to imposing some kind of duty of loyalty on data processors. In my work with Professor Woodrow Hartzog of Northeastern University, I have argued that the solution to the problems of American privacy lies in building trust. Today we face a crisis of distrust. The Snowden revelations created justifiable distrust when Americans and Europeans across the political spectrum realized the scope of largely unconstrained surveillance by the Intelligence Community. The *Schrems* litigation is a further offshoot of this distrust by European consumers, regulators, and judges. Distrust harms everyone—consumers, businesses, and government. It most certainly is bad for business in our modern data-driven economy.

There is a better way than our status quo of distrust. In a series of articles, Professor Hartzog and I have sought to identify the factors that could get us beyond the dangerous fiction of "notice and choice" privacy regulation, and use privacy law to create value for companies as well as protecting consumers. Our trust theory suggests that companies who seek trust must be discreet, honest, protective, and loyal.[31] In a forthcoming article, we give greater detail to a duty of loyalty for privacy law based on the risks of opportunism that arise when people trust others with their personal information and online experiences. Data collectors bound by a duty of loyalty would be obligated to act in the best interests of the people exposing their data and engaging in online experiences, but only to the extent of their exposure. Loyalty would manifest itself primarily as a prohibition on designing digital tools and processing data in a way that conflicts with a trusting parties' best interests. Our basic claim is simple: a duty of loyalty framed in terms of the best interests of digital consumers should become a basic element of U.S. data privacy law. A duty of loyalty would compel loyal acts and also constrain conflicted, self-dealing behavior by companies. It would shift the default legal presumptions surrounding a number of common design and data processing practices, and it would act as an interpretive guide for government actors and data collectors to resolve ambiguities inherent in other privacy rules. A duty of loyalty, in effect, would enliven almost the entire patchwork of U.S. data privacy laws. And it would do it in a way that is consistent with American law and traditions, including its commitments to free expression goals and other civil liberties. A duty of loyalty along the lines we suggest would be a big step for American privacy law, but we think it would be a necessary and important one if our digital transformation is to live up to its great promises of human wellbeing and flourishing. It would also be good for business over the long term. The relationship between privacy and trust has been the subject of a lively and creative academic literature.[32] We also note with optimism that the duty of loy-

---

[30] *New State Ice Co. v. Liebmann,* 285 U.S. 262 (1932).

[31] Neil Richards & Woodrow Hartzog, *Privacy's Trust Gap,* 126 YALE L.J. 1180, 1183 (2017).

[32] Neil Richards & Woodrow Hartzog, *Taking Trust Seriously in Privacy Law,* 19 STAN. TECH. L. REV. 431 (2016); Neil Richards & Woodrow Hartzog, A Duty of Loyalty in Privacy Law, (Sept. 5, 2020) (unpublished manuscript), *https://papers.ssrn.com/sol3/papers.cfm?abstract id=3642217;* Neil Richards & Woodrow Hartzog, *The Pathologies of Digital Consent,* WASH. U. L. REV. (forthcoming 2019), *https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3370433;* Neil Richards & Woodrow Hartzog, *Privacy's Trust Gap,* 126 YALE L.J. 1180, 1183 (2017); Neil Richards & Woodrow Hartzog, *Trusting Big Data Research,* 66 DEPAUL L. REV. 579 (2017); Jack M. Balkin, *Information Fiduciaries and the First Amendment,* 49 U.C. DAVIS L. REV. 1183, 1185 (2016); Jack Balkin & Jonathan Zittrain, *A Grand Bargain to Make Tech Companies Trustworthy,* THE ATL. (Oct. 3, 2016), *https://www.theatlantic.com/technology/archive/2016/10/information-fiduciary/502346/;* Jonathan Zittrain, *Engineering an Election,* 127 HARV. L. REV. F. 335, 340 (2014); Lindsey Barrett, *Confiding in Con Men: U.S. Privacy Law, the GDPR, and Information Fiduciaries,* 42 SEATTLE U. L. REV. 1057 (2019); Ariel Dobkin, *Information Fiduciaries in Practice: Data Privacy and User Expectations,* 33 BERKELEY TECH. L.J. 1, 1 (2018); Cameron F. Kerry, *Why Protecting Privacy Is a Losing Game Today—and How to Change the Game,* BROOKINGS (July 12, 2018), *https://www.brookings.edu/research/why-protecting-privacy-is-a-*

Continued

alty is a topic of debate on this Committee, and we hope that this Committee will take the duty of loyalty seriously as an opportunity to protect consumers, safeguard responsible, sustainable commerce, and allow the United States to once again become a leader in global privacy norms.[33]

Conclusion

Thank you for giving me the opportunity to share my views on the consequences of the *Schrems 2* decision for privacy reform in the United States. In sum, the *Schrems* litigation is a creature of distrust, and while it has created problems for American law and commerce, it has also created a great opportunity. That opportunity lies before this Committee—the chance to regain American leadership in global privacy and data protection by passing a comprehensive law that provides appropriate safeguards, enforceable rights, and effective legal remedies for consumers. I believe that the way forward can not only safeguard the ability to share personal data across the Atlantic, but it can do so in a way that builds trust between the United States and our European trading partners and between American companies and their American and European customers. I believe that there is a way forward, but it requires us to recognize that strong, clear, trust-building rules are not hostile to business interest, that we need to push past the failed system of "notice and choice," that we need to preserve effective consumer remedies and state-level regulatory innovation, and seriously consider a duty of loyalty. In that direction, I believe, lies not just consumer protection, but international cooperation and economic prosperity. Thank you.

BIOGRAPHY

Neil Richards is one of the world's leading experts in privacy law, information law, and freedom of expression. He writes, teaches, and lectures about the regulation of the technologies powered by human information that are revolutionizing our society. Professor Richards holds the Koch Distinguished Professorship at Washington University School of Law, where he co-directs the Cordell Institute for Policy in Medicine & Law. He is also an affiliate scholar with the Stanford Center for Internet and Society and the Yale Information Society Project, a Fellow at the Center for Democracy and Technology, and a consultant and expert in privacy cases. Professor Richards serves on the board of the Future of Privacy Forum and is a member of the American Law Institute. Professor Richards graduated in 1997 with graduate degrees in law and history from the University of Virginia, and served as a law clerk to both William H. Rehnquist, Chief Justice of the United States and Paul V. Niemeyer, United States Court of Appeals for the Fourth Circuit.

Professor Richards is the author of Intellectual Privacy (Oxford Press 2015). His many scholarly and popular writings on privacy and civil liberties have appeared in wide a variety of media, from the *Harvard Law Review* and the *Yale Law Journal* to *The Guardian, WIRED,* and *Slate.* His next book, Why Privacy Matters, will be published by Oxford Press in 2021.

The CHAIRMAN. Well, thank you all for excellent testimony. I wish the testimony had made me more optimistic about a solution, but I think it just confuses me a little more and points out the complexity of what is before us. Ms. Espinel, your organization submitted an amicus, but in a few words or less, were you—whose part were you taking and were you disappointed or delighted at the decision?

---

losing-game-today-and-how-to-change-the-game/; Ian Kerr, *The Legal Relationship Between Online Service Providers and Users,* 35 CAN. BUS. L.J. 419 (2001); Daniel Solove, THE DIGITAL PERSON (2006); Richard S. Whitt, *Old School Goes Online: Exploring Fiduciary Obligations of Loyalty and Care in the Digital Platforms Era,* 36 SANTA CLARA COMPUTER & HIGH TECH. L.J. 75 (2019); Kiel Brennan-Marquez, *Fourth Amendment Fiduciaries,* 84 FORDHAM L. REV. 611, 612 (2015); Lauren Scholz, *Fiduciary Boilerplate,* J. CORP. L. (forthcoming 2020); ARI WALDMAN, PRIVACY AS TRUST (2018); Ari Ezra Waldman, *Privacy As Trust: Sharing Personal Information in A Networked World,* 69 U. MIAMI L. REV. 559, 560 (2015); Ari Ezra Waldman, *Privacy, Sharing, and Trust: The Facebook Study,* 67 CASE W. RES. L. REV. 193 (2016); Christopher W. Savage, *Managing the Ambient Trust Commons: The Economics of Online Consumer Information Privacy,* 22 STAN. TECH. L. REV. 95 (2019).

[33] See Neil Richards & Woodrow Hartzog, *A Duty of Loyalty for Privacy Law,* forthcoming 2021, available at *https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3642217.*

Ms. ESPINEL. We were taking the part of cross-border data transfers. So, yes, we were invited to be an amicus along with the U.S. Government and the European Commission in the case, and we felt it was important to do so for two reasons. The first is because our members believe so strongly in privacy protection, but the second is because cross-border data transfers are not just a software issue or a tech issue, they are an issue for every company, no matter the size, no matter the sector.

The CHAIRMAN. Were you advocating for the arrangement to be upheld?

Ms. ESPINEL. Yes, we were advocating for it to be upheld. But I do emphasize this point, not so much on behalf of our companies, but on the behalf of the customers of our companies, because they are—it is companies across the United States that rely on cross-border data transfers, and so one of our main points to the court was that this would have far reaching ramifications for the U.S. and the European economy if it were invalidated.

The CHAIRMAN. OK. And that certainly turns out to be the case. Mr. Swire, what is significant about January 20 other than it is inauguration day? There is no enforcement that kicks in beyond that?

Mr. SWIRE. Well, there is no enforcement that kicks in. In speaking to at least one litigator, I have heard an ominous prediction that there may be court orders in Europe on one or more major U.S. tech companies by that time, which would be—that would grab some headlines and attention to the issue if court orders like that came out. And there is an opportunity, it seems, for Mr. Sullivan and the hard working people who are working on those issues currently, in my dream world, to imagine trying to get some kind of at least short term interim way to have something happen.

When brand new people come in, it takes a little while to get up to speed. I am assuming there is new people coming in. And so the very up-to-speed people who are there now have a particular opportunity to do something that would then lead to easier chances for better some things after that date.

The CHAIRMAN. OK. There is no grace period. There is a decision that went into effect immediately.

Mr. SWIRE. Right. Correct. Yes.

The CHAIRMAN. Are companies being hauled into court right now?

Mr. SWIRE. There are numerous—I don't know—I am sorry. There are multiple lawsuits in different countries that are happening right now, yes.

The CHAIRMAN. OK, but do I take it that your position before the decision is that the Privacy Shield agreement should be upheld and left in place? Is that your position?

Mr. SWIRE. I believe the U.S. had essentially equivalent protections and should have been found that way, but the court disagreed with that.

The CHAIRMAN. It sure did. And then, Professor Richards, you assisted the Irish government in this case, is that right?

Mr. RICHARDS. That is correct, sir.

The CHAIRMAN. Good. And, what was their position with regard to whether this should be upheld or not?

Mr. RICHARDS. So the position of the Irish Data Protection Commissioner—I was an independent expert, as was Professor Swire. Under Irish procedure, experts tend to not to be, to use the colloquial term, hired guns the way they tend to be in American litigation. So we took an oath to give the evidence that we would give, say if Facebook or Ireland had retained us. But the Irish Data Protection Commissioner took the position that there were sufficient doubts about the legitimacy of the Privacy Shield, of standard contractual clauses and by extension Privacy Shield under European law, that she chose after an investigation to seek a referral to the European Court of Justice, which made the ultimate determination.

The CHAIRMAN. OK, now Mr. Phillips, was it you that—this is all good testimony, by the way. Excellent job on a complex issue. Who was talking about the comparative surveillance done in Europe? That was you, was it not?

Mr. PHILLIPS. Senator, I did refer to that.

The CHAIRMAN. OK, and are you saying that basically when it comes right down to it, there is not really that much difference in the way our intelligence services surveil as compared to Europe?

Mr. PHILLIPS. Senator, there have been a number of studies by authoritative lawyers and academics here and in Europe, and the bottom line has been that the practices that we engage in from a National Security perspective afford just as many, if not more, rights to U.S. citizens as rights afforded by domestic law in member states of the EU.

The CHAIRMAN. And it seems to me that in resolving this matter, that is going to be quite the sticking point.

Mr. PHILLIPS. I think that is an important consideration, absolutely.

The CHAIRMAN. Well, thank you all. And there will be other rounds of questions, but this has been a great panel. Senator Cantwell.

Senator CANTWELL. Thank you, Mr. Chairman. Senator Peters, do you need—do you have a time constraint? OK, thank you. Well, this has been very helpful, I think. And again, appreciate the opportunity for the hearing, Mr. Chairman, and the witnesses. Mr. Richards, I am struck by this issue of trust and distrust because I think there is so much of that in practically every issue. But clearly, this one is a thorny one. And so we do have to figure out a way to build trust again because we are in the digital age and this won't be the last issue or the last time we have to address this.

This is going to continue far into the future. This is the era that we live in. And so I appreciate you mentioning our efforts here in the Senate and our colleague, Senator Schatz's effort on duty of loyalty too because I think that plays into trust and the environment. On those factors that you mentioned, appropriate safeguards, rights, and enforcement, Mr. Richards, I am interested in this larger—so that is a good framework, very important framework, and I believe in that framework. I think that is the essential aspect of the framework, but over here, somewhat out of control of Senator Wicker and I, is Government surveillance.

And I want to hear what Mr. Richards, you say and other people say about how we build trust on tackling our most important Na-

tional Security issues. So it is almost like industry now is going to be hamstrung. We could fix these issues, appropriate safeguards, rights, and enforcement, but over here is going to be this large issue about data gathering by the Government. And I want us to figure out how we are going to move forward. So two examples, Senator Collins and I worked with the former Secretary of Homeland Security, Jay Johnson, to implement overseas borders. That was hard because you are basically doing border security at overseas airports, but no one wanted to turn over—you know, the United States was not going to get access to European or whatever country we were in data, but yet we had to figure out a system where we were both going through potential security risks on our own data.

We figured that out. I know, for example, on some of the National Security issues, there is alliance on software. So I am pretty sure both in Europe and the United States, there are foreign countries working together where on software security. So we figured it out. So, Mr. Richards, what do you think those security surveillance issues are that really aren't even within our Committee jurisdiction, but that we have to figure out how to build trust on so that we can resolve this issue so that we don't have business in the digital era hung up on digital trade because basically our two governments can't figure out how to work together.

And if we can't figure out how to work with the Europeans, I got news for you, we got problems. Like, we have got to figure out how to work with the Europeans and to figure this out. So, Mr. Richards, do you have a thought on that?

Mr. RICHARDS. I do, Senator. I mean, obviously, this is a very difficult problem. The question you have asked me, to solve international surveillance cooperation in less than 2 minutes. But I will give it my best shot. I think some of the other speakers, some of the my co-panelists mentioned the importance of privacy protections flowing with the data, and also the importance, I think Commissioner Phillips mentioned this, the importance of countries with shared values having shared protections.

And I think it absolutely should be possible, I realize in Washington should is often a very dangerous word, but I think that it should be possible for countries, for the EU, the United States, the country of my birth, the United Kingdom, with shared commitment to the rule of law, shared commitments to freedom of expression and privacy and democracy, shared strategic and economic interests to cooperate, to extend rights of redress to each other's citizens the way that the U.S. Government did with the passage of the General Redress Act, amending the Privacy Act in 1974 in order to try and save Privacy Shield in the spring of 2017. I think extension of rights and also cooperation, a coalescing on those privacy protections that should travel with the data is.

Unfortunate, the United States used to be the leader on commercial privacy in the early 1970s. It sort of abdicated that to Europe. And now that the GDPR, fair information practices model that the Europeans have, is the emerging global market norm. But if the U.S. cooperated on that as well, I think it could go a great deal toward solving the broader problems of international cooperation on surveillance.

Senator CANTWELL. I just want to follow up, so—I actually think we might be able to achieve that. But then what are we going to do about the fact that we don't control—well, Senator Wicker and I do have votes on this in the larger body, but we don't control these agencies and we certainly don't control executive orders and the Presidential Executive Order. All we can do is fight it and say that we think it is too broad. So how—I am in agreement, we can solve our commercial issues.

I just don't know if we are still, if the commercial industry is still going to get tethered to a national policy by an Executive Branch that thinks that we need to go further. Personally, I think we need way more transparency on the FISA court. Look, these are—we blurred the line in the Patriot Act and we just, we have got to do more due diligence here. So, thank you, Mr. Chairman.

The CHAIRMAN. Yes. You have outlined a serious stumbling block, Senator. I believe Senator Blackburn is next. Are you there, Senator?

STATEMENT OF HON. MARSHA BLACKBURN,
U.S. SENATOR FROM TENNESSEE

Senator BLACKBURN. Yes, I am.

The CHAIRMAN. You are recognized for 5 minutes.

Senator BLACKBURN. Thank you, Mr. Chairman. And thank you to our witnesses for being here and for the opportunity to have this hearing today. Privacy Shield, as everyone is fully aware, is something that continues to come up. We have got dozens of companies in Tennessee that would be impacted. I had pulled a list and it is interesting that the wide range of the companies that would be impacted, adversely impacted without an agreement.

And everything from a vitamin company to a software company, to the Dollywood Foundation, to the Country Music Association. So as we talk about trade, as we talk about commerce, this is something that is important. I do appreciate that Senator Cantwell brought up the issue of trust and distrust as we look at this issue. But resolving it and getting something in place is vitally important. So, Mr. Sullivan, let me come to you first.

Let's say we are not able to negotiate an agreement. If we do not get an agreement, then it seems like that data localization may become the new norm. So I want you to speak to what would be an adverse outcome?

Mr. SULLIVAN. Thank you, Senator, for the question. I guess at the outset, let me make clear, you know, I alluded to the three successful annual reviews that we have had since 2017, where we sat down with the European Commission, the European Data Protection authorities, and those are three very successful internal reviews. And during that period, since that period, before during after those reviews, we have developed very constructive, excuse me, and positive working relationships with our partners in Europe.

I do want to note a couple of points. You know, we have been talking about the *Schrems II* litigation since well before the third annual review, which took place last October. There has been a long-running argument about contingency planning. We have been in constant regular contact with the Commission since the ruling

on July 16. Secretary Ross has reached out to a number of high ranking EU officials.

And, you know, we are working urgently to resolve this crisis because Privacy Shield, as you alluded to, is the most cost effective and straightforward mechanism for SMEs. And as I think I said, nearly 70 percent of the participants in Privacy Shield are SMEs. And that is—again, that is across all sorts of industries. We are not, again, talking just about digital companies or big multinational tech companies. So, you know, obviously our first priority is privacy——

Senator BLACKBURN. We are not talking about just digital companies. I just went through the list. You know, you have got Dollywood Foundation and the Country Music Association, CISAC, a vitamin company, all of these different Tennessee companies. But talk about data localization. And if we don't get something, what does that mean and the impact? And then I would like to have Ms. Espinel and others weigh in when you finish your comment.

Mr. SULLIVAN. Of course. So, again, Privacy Shield, I just want to be clear, 70 percent are SMEs with fewer than 500 employees. So we are extremely sensitive to that. And we do recognize to your point, you know, in the hopefully unlikely situation where we do not arrive at a new arrangement or an enhanced Privacy Shield, you know, there are other mechanisms. Obviously, the court upheld SCCs. We have worked with our inter-agency partners to put out a White Paper to hopefully help companies make these case by case assessments.

On your question, with respect to data localization. That is a very significant concern for us. My team has been engaged with Europe, but also in countries around the world on this issue. And quite frankly, it is not a perfect solve. It is exceedingly expensive, even for our large companies that will effectively freeze out SMEs in many of the companies that you are talking about from access in the EU market.

And quite frankly, it doesn't work at the end of the day. It is simply—beyond the expense factor, trying to keep EU personal data in Europe effectively undermines the business models of the vast majority of companies that operate this way internationally. And so that is not, at the end of the day, a viable solution. And if I could——

Senator BLACKBURN. Ms. Espinel—I don't want to run out of time. Do you have anything to add on that?

Ms. ESPINEL. I would say that the organizations that he talked about music, country music—the organizations that you mentioned, the Country Music Association, the vitamin company, they are on that list they were certified under the Privacy Shield because they have employees or customers or suppliers in Europe. And if they—if data localization goes into place and they are not able to access that, that means that they are not going to be able to operate effectively either.

They will be operating at greatly increased cost or they won't be able to operate in Europe at all. So the implications of data localization are very significant for those organizations, but for organizations including many small and medium sized businesses across the United States.

Senator BLACKBURN. Right. You are changing their business model through no fault of their own. Alright, Mr. Phillips, anything to add?

Mr. PHILLIPS. I agree with what both of my co-panelists said. I also just want to add, data localization isn't good for privacy. It isn't good for data security. It doesn't serve all of these other functions in addition to all the cost that it imposes on businesses and nonprofit organizations.

Senator BLACKBURN. Alright. Mr. Richards?

Mr. RICHARDS. Sorry, Senator, I was struggling with my mute button. Data localization absolutely would be bad, and I think the key, as a number of the other witnesses have pointed out, is to find some way to harmonize the law. The Europeans, as Professor Swire pointed out quite correctly, treat this as a matter of constitutional law.

They believe that just as when they come to the United States, they may go to Dollywood on vacation, that they expect that their constitutional rights travel with them just the same as you or I would expect that our constitutional rights would follow us if we went to Europe. And I think because the U.S. is in a sense importing the data like a tourist, the Europeans expect that their rights are guaranteed.

And I think this is not—this is a hard problem, but this is not an irresolvable problem because of our shared traditions and commitments to the rule of law, democracy, and fundamental rights.

Senator BLACKBURN. Mr. Chairman, thank you. Yield back.

Senator THUNE [presiding]. Senator Blumenthal is up.

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

Senator BLUMENTHAL. Thanks, thanks very much, Senator Thune. As you probably know, all of you, this committee has spent a good deal of time and effort over the last two years on consumer privacy, and I appreciate the leadership of the Chairman and Ranking Member. And I am grateful for the collaboration of Senator Moran.

We have worked together on this issue, given California's passage of Proposition 24 and the change of Administration. This is an area where I think we can make significant bipartisan progress in the next Congress, obviously not this one. I have been fighting for consumer privacy for many, many years as Attorney General before I assumed this office and I want to see a strong Federal law enacted. And I believe it is possible. This absence of consumer protections is part of the reason we have this dispute with the European Union.

The United States and the EU need and have needed a Privacy Shield in the first place because the EU determined that our consumer privacy protection in this country are inadequate, as a safeguard to personal data. So our lack of consumer protection in this country for Americans, private data, also harms American businesses that want to operate in Europe.

All five of you are respected privacy experts and all of you called for a Federal consumer privacy law. I thank you for your advocacy. And I would like to know more definitely from each of you, what

role does the United States' lack of consumer privacy law play in our negotiations with Europe on cross-border data transfers? Would having a consumer privacy law for the United States help end the cycle of Europe striking down data transfer agreements? Maybe begin with you, Mr. Sullivan.

Mr. SULLIVAN. Thank you for that question, Senator. Just a couple of points, if I could. The adequacy model that has been adopted by the EU since about 1995 has to date yielded about 12 adequacy determinations. There are only 12 jurisdictions in 30 years that have been acknowledged as adequate by the EU. At the same time, there is today no globally accepted standard or definition of data privacy and no multilateral agreement on these issues. And so I think that is going to continue regardless of whether or not there is an omnibus Federal privacy law that will remain to be seen.

But specifically with regard to the situation we are in after *Schrems II,* that ruling focused exclusively on Government access to data. And the court did not in any way question Privacy Shield's protections with regard to commercial collection or uses of data. And while I think that potential Federal data privacy legislation would likely be very well received by the EU, it will not address the immediate concerns that we are dealing with around the National Security issues cited by the court in *Schrems II.* Again, I think, you know, I will speak in my position with the International Trade Administration.

We are seeing a proliferation of different national laws around the world. Some are taking their inspiration from GDPR. That is not a guarantee of adequacy. You have a law in India, for example, that sought to emulate GDPR in many ways. Each Nation has different cultural traditions, legal traditions, backgrounds, priorities. Brazil, similarly. So while I think it could help atmospherically and it would probably be very well received by our friends in Europe, it is not a guarantee. Thank you.

Senator BLUMENTHAL. Thank you. Mr. Phillips.

Mr. PHILLIPS. Thank you, Senator, for the question. Let me just begin by agreeing, of course, the *Schrems II* decision is about National Security. There is no guarantee that would come from a privacy law. And as I said in my written statement in my oral testimony, while we don't have a law, I think that our privacy enforcement is better than any in the world and more impactful than any in the world. That said, I do think a law will help.

I think first, if we are going to do the interoperability between countries of data flows, having one law is a better way to handle that on an international basis rather than having to deal with different jurisdictions. The second, as we have heard from all the panelists atmospherically, I think it does help. Third, I think there are aspects of a privacy law that you and your colleagues, and I thank you for your leadership on this, have contemplated that would help a lot of entities.

For instance, removing limitations on the FTC's jurisdiction with respect to common carriers and nonprofits will allow those entities to participate in whatever new Privacy Shield resolution that we might have because all of a sudden their obligations would flow through us. So I do think it would be a helpful thing.

Senator BLUMENTHAL. Thank you. Ms. Espinel.

Ms. ESPINEL. Senator Blumenthal, thank you for the question. I just want to thank you for your years of leadership and dedication on privacy legislation. So I agree. I believe that privacy legislation would be a very positive signal to the Europeans. I want to emphasize that I think we need Federal privacy legislation regardless of the situation that we are in, even if the Privacy Shield had not been invalidated.

We need it for U.S. citizens so that you have strong, enforceable privacy protections across the United States, and strong obligations on companies. But I also believe that it would be a positive signal and would be a benefit to the negotiations.

Last, I just want to say I also believe strongly and would encourage this committee to think about the long term issue of whether or not we can reach some sort of consensus with at least like-minded countries that share our values on intelligence gathering practices, because I believe that is really critical to finding a long term sustainable solution.

Senator BLUMENTHAL. Thank you very much.

Senator THUNE. Thank you, Senator Blumenthal.

Senator BLUMENTHAL. Thank you.

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

Senator THUNE. Commissioner Phillips, after the passage of the EU's GDPR, the flow of data between the U.S. and the EU has become less stable and subject to much debate. Would a single national data privacy law in the United States be beneficial to help resolve some of the policy differences between the EU and the United States?

Mr. PHILLIPS. Yes, Senator.

Senator THUNE. And Mr. Sullivan, do you agree with that?

Mr. SULLIVAN. Yes, short answer.

Senator THUNE. Short answer——

Mr. SULLIVAN. The short answer is yes.

Senator THUNE. OK, good. Mr. Sullivan, what kinds of businesses and industries rely upon the Privacy Shield framework? And can you talk about the importance of the need to transfer data across borders?

Mr. SULLIVAN. Of course. So at the time of the ruling on July 16, there were nearly 5,400 companies. As I think I have said before, nearly 70 percent of those companies participating in the Privacy Shield program were small and medium sized enterprises with fewer than 500 employees.

The reason for that was because it was a cost effective mechanism, far less administratively burdensome and costly than some of the other options, such as standard contractual clauses or binding corporate rules, which are largely used by large multinationals. The participants in Privacy Shield were again from across industry.

We are talking about small manufacturers, we were talking about agricultural producers, other small businesses in a variety of industries. So, again, just I know I am a bit repetitive, I want to underscore we are not simply talking about large multinational tech companies or digital firms. Everyone has to transfer data

these days across the Internet, H.R. records, for maintaining their international networks, etc. So it is a broad swath of U.S. industry.

Senator THUNE. Thanks. Commissioner Philips, at a hearing earlier this year Chairman Simons stated that the FTC intends to make companies fulfill the promises made under Privacy Shield. Has the Commission brought enforcement actions with regard to Privacy Shield since the time the European Court of Justice invalidated the EU-U.S. Privacy Shield?

Mr. PHILLIPS. Senator, I am a little bit lost on the timing, but I believe the answer is yes in the RagingWire case. The enforcement that we do on Privacy Shield is under our Section 5 deception authority. And what it means in the main is if you are making material statements to consumers and you violate those statements or, right, you are deceiving those consumers, we can go after you. So representations that they are making with respect to participation in, or following the guidelines of the Privacy Shield, come under that rubric. And we are going to continue to enforce against companies that don't live up to their commitments.

Senator THUNE. Good. Ms. Espinel, the cross-border transfer of data is, as has been pointed out, vital to our economy. As the U.S. and the EU work to develop a successor, I should say, to the Privacy Shield, are there safeguards the U.S. should be giving consideration?

Ms. ESPINEL. Thank you. So I think in terms of the negotiation on the enhanced Privacy Shield, I don't believe we need a total overhaul of the Privacy Shield. I think there are some targeted reforms that could address some of the issues that were raised specifically by the court. And we are very supportive of the work that the Department of Commerce and the U.S. Government and the European Commission have been doing together. I will say, as I have said before, I think longer term, having the United States work with a group of democracies that share our values to try to come to a consensus on intelligence gathering practices is critical to long-term sustainability.

But in terms of the immediate, urgent, short-term need for an enhanced U.S. Privacy Shield, I think there are targeted reforms that I believe, obviously Mr. Sullivan could speak better to this, but I believe could be addressed in the negotiations between the United States and the European Union.

Senator THUNE. Mr. Swire, what effect would the emergence of data localization requirements in the EU have on Americans' National Security?

Mr. SWIRE. On National Security—well, in my testimony I refer to previous work that I have done with others on data localization, and we hope to have more information about that by the end of the month published. For National Security, one of the problems would be cybersecurity in the following way. When currently, if you are trying to figure out where the bad guys are coming from, you have global flows among the defenders to make sure that we are getting a good view of where the bad guys are coming.

And if the data cannot come from Europe to the rest of the world, then the bad guys know they just have to route it through Europe. So we are going to have a discussion at the National Academy of Sciences on December 11 specifically about the effects on

cybersecurity, which affects U.S. National Security, affects corporate security. And this is something that has not been brought up but is really deserving a lot more attention, the effects on cybersecurity.

Senator THUNE. Mr. Chairman, thank you.

The CHAIRMAN. Thank you, Senator Thune. Senator Peters.

STATEMENT OF HON. GARY PETERS,
U.S. SENATOR FROM MICHIGAN

Senator PETERS. Thank you, Mr. Chairman. Mr. Swire, I want to follow up on the question that Senator Thune asked you, because it seems like if eliminating the Privacy Shield, that that could possibly result in the global adoption of data localization, and I know data localization is the hallmark of both Russian and Chinese efforts to centralize and surveil valuable streams of data, something we always have to be conscious of.

And I am Ranking Member of Homeland Security Committee here in the Senate, and I am certainly committed to protecting National Security. And as you were saying, it is something that we need to focus on because it has potential to undermine our security interests. What specifically should we be doing to address this because I am concerned about it?

Mr. SWIRE. Well, one thing is to have people in Europe understand how serious and how difficult it is to even try to build data localization. It is a much more thoroughgoing revision of every company's IT system than most people have seen. In a 1998 book, we have had multiple chapters about data localization even back then with about 40 categories of serious effects. And that is linked to in my testimony. And one of the examples is the global financial system, which we rely on for so many things, including, you know, ongoing secure commerce.

There are massive data flows of personal data every day between countries for regulators to oversee banks, among other things. And if there is really data localization, we lose the ability to have an integrated global financial system. That all by itself could be a hearing that really was worth a lot of attention, perhaps in a different committee, but it illustrates how thorough the interruption would be if really data localization happens from Europe.

Senator PETERS. Right. Well, thank you. My next question relates to small business. Ms. Espinel, I would like to ask this question of you. And I think, Mr. Sullivan, you were dealing with small business. I am going to follow up with a question for you related to this too. Because I was walking in so I wasn't sure of the question, but your answer is probably related to what I want to talk about. But in our increasingly connected world, certainly of small businesses like manufacturers or retailers as was mentioned, rely on the free flow of information.

In fact, 70 percent of the companies that have certified under Privacy Shield are small or medium sized businesses, and they simply can't afford to store data overseas, especially those small businesses. Of those companies we have identified, 993 companies in Michigan alone fall into this category. So if you could tell me the lack of certainty on international data transfers, how is this going to impact small businesses immediately? And are there steps that

we can take here in Congress to address it? How do we mitigate that?

Ms. ESPINEL. So I think it is an immediate concern. I mean, I think it is worth noting that there are other transfer mechanisms that are still in place. So the standard contractual clauses were left in place by the court and we are very pleased that that is the case. So there are still other transfer mechanisms between the United States and Europe. That said, the Privacy Shield was the simplest and the least costly of all the transfer mechanisms.

So for small businesses in particular, having the Privacy Shield invalidated is a real concern. Standard contractual clauses are positive in the sense that they can offer very strong privacy commitments to consumers, but they are more complicated, they are more resource intensive, so they are more difficult by definition and therefore more difficult for small businesses. And as you pointed out, small businesses are 70 percent of the companies that are certified under the Privacy Shield.

And so, we believe that having an enhanced EU-U.S. Privacy Shield, having a Privacy Shield agreement back in place that small businesses can take advantage of, is of critical importance.

Senator PETERS. Thank you for that answer. And Mr. Sullivan, I know you are concerned about this as well. And my focus—you know, U.S. small businesses are U.S. innovation and our innovators that really rely on these data flows, particularly when you think of technologies like artificial intelligence and the need for data sets to deal with that.

Talk to me about some of the legal uncertainty for international data transfers that are going to impact tech startups, particularly in the innovation sectors. If so, how? And any other ideas of how we need to deal with that?

Mr. SULLIVAN. Certainly, Senator, and thank you for the question. We have all talked about how important Privacy Shield is for SMEs. We have just heard again about how difficult some of the other options SCCs and BCRs, binding corporate rules, which can take up to a year and cost upwards of $1 million, which is just not an option for small startups, tech or otherwise. Which is why, you know, we are working so urgently to develop an enhanced Privacy Shield to address the enormous uncertainties that now exist and do so quickly because of these uncertainties.

You know, some can avail themselves of SCCs. And although there are now some significant questions about their viability, we have put out a White Paper to help companies so that they can help or they can make these case-by-case assessments that have since been required by the *Schrems II* decision, before they send data to the United States. But I think, you know, one thing I do want to touch on that others have spoken to, you know, we have heard a lot today about the need for perhaps a broader discussion among like-minded democracies. I do want to emphasize that we have, my team at the International Trade Administration in concert with others across the interagency, have been engaged with the European Union and other democratic countries in a number of different multilateral discussions about developing principles and common practices.

There is an effort underway right now in the OECD to just to do just that around, can we arrive at common principles when it comes to Government access to data? And in our view, it is critical that democracies come together to articulate shared principles, primarily not exclusively, to help make clear the distinction between what democratic societies do and how we respect civil liberties and the rule of law versus what we see authoritarian countries do with their growing surveillance ambitions to surveil, manipulate, and control their own citizens and others around the world with zero regard to privacy or civil liberties.

And so we are really approaching this situation, and again SMEs are a priority for us. Many big companies can avail themselves of all the different mechanisms that are step one with Privacy Shield. The other thing I do want to note with Privacy Shield, you know, if we get it back up and running soon, what Privacy Shield did was it took the protections and redress mechanisms in the context of Government access to data and said these apply not only to companies that participate in Privacy Shield but to data transfers pursuant to any EU approved data transfer mechanism.

Now, since the ruling, what you have is a situation where companies are now stuck with this incredibly onerous burden of having to do case-by-case assessments. If we get a Privacy Shield framework back in place, that will alleviate all companies of all sizes of this onerous burden of having to do these case-by-case assessments of countries' National Security regimes. 1

And so I just want to emphasize we have a number of different work streams on this beyond just the discrete issue of trying to come up with enhancements on Privacy Shield. Thank you.

Senator PETERS. Thank you so much. Thank you, Mr. Chairman.

The CHAIRMAN. Thank you, Senator Peters. Ms. Espinel, lawsuits are being pursued even as we speak against your member companies. Is that correct?

Ms. ESPINEL. I am not aware of any lawsuits that are being prepared against my member companies, against the enterprise software industry that I represent, and it is helpful and we were pleased that other transfer mechanisms like the standard contractual clauses were left in place by the European Court of Justice. And our companies use the standard contractual clauses to transfer data. However, as we have discussed, standard contractual clauses are much more difficult, much more costly, more complicated, resource intensive way of transferring data.

And therefore, we believe it is urgent that a new Privacy Shield be put back in place, both for the benefit of the small and medium sized businesses which we have discussed quite a bit because of the difficulty and resource intensive nature of the standard contractual clauses, but also because even for the standard contractual clauses, they will be more stable and more solid if there is an enhanced U.S.-EU Privacy Shield agreement.

The CHAIRMAN. Sure. Well, who can enlighten the Committee on the degree to which lawsuits are being filed now since there is no grace period? Mr. Swire?

Mr. SWIRE. I could try a little bit. There has been public reports in Ireland of ongoing court proceedings, specifically about Facebook. There have been suits filed———

The CHAIRMAN. In Irish courts?
Mr. SWIRE. Yes, sir.
The CHAIRMAN. OK.
Mr. SWIRE. They are national courts that—currently they are not being appealed up to the European wide court system yet. There have been public reports about a suit in Germany against Amazon. And in talking to one litigator who works specifically in that area, I was told there are other suits, but I don't know exactly what the details are.
The CHAIRMAN. In those cases, do insurance carriers step forward and represent the companies? Defend?
Mr. SWIRE. I am not aware of that—is not—a lot of it has to do with company conduct and whether the conduct is lawful or not. And so large companies would probably defend themselves.
The CHAIRMAN. So well, OK.
Mr. SWIRE. But they are facing fines——
The CHAIRMAN. Is it possible for companies to purchase insurance coverage to mitigate against these types of actions?
Mr. SWIRE. I am aware of many kinds of cybersecurity protection that are in place for data breaches. I have not heard, and I work a lot in the sector, of any significant insurance for fines for privacy violations.
The CHAIRMAN. OK. Senator Schatz, are you there? I think Senator Schatz——

STATEMENT OF HON. BRIAN SCHATZ,
U.S. SENATOR FROM HAWAII

Senator SCHATZ. Sorry, Chairman, I am here.
The CHAIRMAN. Yes, sir. You are recognized, sir.
Senator SCHATZ. Thank you, Chairman. And thanks to all the panelists for a really constructive hearing. I want to start with Mr. Richards. You know, the *Schrems* decision highlights why the United States needs a strong data privacy Federal statute. And I, of course, believe that we need a duty of loyalty and care in Federal law. And I would like you to comment on how duties of loyalty and care could complement the privacy principles in the Privacy Shield and European privacy law without doing violence to our conception of freedom on the Internet and the United States?
Mr. RICHARDS. That is a great question, Senator. If I could if just respond to the last question the Chairman asked about lawsuits. In my written testimony, I did cite an Irish newspaper which is reporting on the Facebook proceeding where the data protection commissioner has proceeded to try and pursue the *Schrems II* ruling to stop data flows to from Facebook Ireland to Facebook U.S., which it is not the kind of risk you can really insure for if the data flows are the business itself.
With respect to your—Senator Schatz, and thank you very much for asking, one of the problems with the European approach, which incidentally was invented, as I am sure the Senator knows, by the U.S. Government in a Department of Health, Education and Welfare in 1973—so these GDPR rules that we are talking about, as if they are they are foreign law, were actually invented by the U.S. Government. They tend to be procedural. They tend to say basically, here is how you process data. If you want to do it, these are

the steps you have got to go through. But by and large, they provide a pathway for doing so.

And while data protection rules notice choice, access, consent in appropriate circumstances, legitimate interests, onward transfer are going to be a necessary part of any robust transatlantic or domestic or European framework, what we need to have are substantive rules. Senator Schatz, you said in the September hearing I believe to Commissioner Kovacic that a duty of loyalty isn't that big of a burden because good companies already know how good business means being loyal to their customers.

And actually a duty of loyalty that requires putting your customer's interests ahead of your own in the short term is good for sustainable long term business. And actually, the companies that are being loyal when they are not required are actually at a competitive disadvantage from the bad guys that act in ways that are disloyal, that manipulate their customers that mislead them, that send them misinformation, that expose them to insecure and unfair data practices.

Senator SCHATZ. So I think you make a really important point. And I, for the life of me, don't understand the resistance to duty of loyalty other than Government relations folks feel that their job is to kill everything and lawyers feel that anything that may be unclear and needs to be elucidated over time or even a statutory obligation that has to be elevated to the board level is inherently a risky proposition.

But as you are—as we see, doing nothing is riskier than anything for your customers, for the Shield problem, and for the prospect of 50 different states enacting 50 different statutory frameworks. And so it seems to me that the cleanest way to move forward is not just to enact—of course, everyone thinks they are the cleanest way to move forward is to enact their legislation. But it does seem to me that we have to legislate at the conceptual rather than procedural level and empower expert agencies to implement the statute through rulemaking or even the adjudication of individual cases. So talk a little bit more about how notice and choice would be insufficient, not just from a consumer protection standpoint, but from the standpoint of solving our Shield problem?

Mr. RICHARDS. Notice and choice are wholly inadequate. They basically are—the way they have been implemented in U.S. law, with apologies to Commissioner Phillips and his agency, which has done fine, fine work with limited tools over the years, but the notice and choice framework has been a catastrophic failure. The notice that consumers receive is fictitious. Do you read privacy policies? Right. There was there was a study that it would take 76 days to read all the privacy policy, just to read them, of the websites that we encounter in a year———

Senator SCHATZ. I just think—I think that everything on my—I was just setting up Apple TV and I just agreed to everything without reading it like everybody does.

Mr. RICHARDS. So do I, Senator, and that is precisely the point. We have no choice and that is the other fault with notice and choice. If we want to participate in the modern world, we have to accept these terms and conditions as they are given, as they are unread. And often we don't have a choice at all. In the pandemic,

we may have a choice over our streaming service but we don't have a choice over a cable company. We don't have a choice over the learning management system or the video conferencing system that our children's schools are using.

And so what has happened is that notice and choice have been an insufficient check on bad actors in the market and they have given consumers resignation. And it dumps the work onto consumers, work they cannot possibly hope to achieve, and then it performs a masterful trick of making consumers feel bad and blame themselves for consenting to privacy policies when they didn't actually have a meaningful choice in the first place. Sorry, sir.

Senator SCHATZ. Thank you. Let me let me just move on to one final question for you, Deputy Assistant Secretary Sullivan, on the transition. Have you been meeting with the Biden, Harris transition team? What is the frequency of those meetings? What is the extent of your sharing information as we move into the next phase and a transition to a new Administration?

Mr. SULLIVAN. Thank you, Senator, for that question. As I noted at the outset, I oversee the Office of the Digital Services Industries. We have three teams. I will tell you that each of those teams has met on multiple occasions with transit at the agency review team at Commerce. We also prepared a transition memo that was intended to bring everyone up to date on the state of play with the litigation and the various lines of work we have, again, around Privacy Shield, standard contractual clauses, our multilateral efforts, and a variety of different venues be it OECD, the G20, etc. So my understanding is they are being kept fully apprised of our activities and our engagement with the Commission, the EDPB, and others and the member states in Europe.

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

The CHAIRMAN. Thank you, Senator Schatz. Let me ask you, Professor Richards, where is there a working duty of loyalty in place in law somewhere that we can look to?

Mr. RICHARDS. That is a great question, Senator. As an academic, I feel obligated to plug an article that Dr. Hartzog and I have written called "A Duty of Loyalty for Privacy Law" that explores this in great detail. But to answer the question very specifically, duties of loyalty have been a part of the Anglo-American common law for centuries. We often see them in fiduciary relationships and in corporate law. We tend to see that whenever there is vulnerability, whenever one party exposes itself to another for combined interests. And frankly, Senator, Mr. Chairman, that is precisely what we see with large platforms in the Internet economy. We need to have use it to expose ourselves to these companies in order to send e-mail, to engage in transcontinental videoconferencing like we are doing right now, to educate our children, and for so many other ways.

I think one other place we can look for duties of loyalty, I think it is very interesting and very gratifying and encouraging to me that all three of the pending bills that were introduced, bills that we have talked about in today's hearing, your SAFE DATA Act, Senator Schatz's Data Care Act, and Ranking Member Cantwell's COPRA, all of them either talk about loyalty, or in the case of Title

II of your bill, provide loyalty like protections against manipulation, against filter bubbles, against algorithmic discrimination, and against the manipulative—and against experimentation and manipulative use of design against consumers.

The CHAIRMAN. And the point that I would make is that when we are able to be specific in those instances, then we are getting somewhere, but beyond that, it is hard actually to define such a duty. I am going to let you expand your answer on the record, if you would like. And I may submit some questions for the record. This study that you and Dr. Hartzog did, when was that published, sir?

Mr. RICHARDS. It has not yet been published, but it has been circulating on and on the website where academic work is. A draft has circulated since the summer.

The CHAIRMAN. Can you circulate it to somebody on my staff?

Mr. RICHARDS. I believe I already have, but I would be delighted to do it again, sir.

The CHAIRMAN. I would much appreciate that. Senator Scott.

STATEMENT OF HON. RICK SCOTT,
U.S. SENATOR FROM FLORIDA

Senator SCOTT. First of all, I want to thank Chairman Wicker for hosting this hearing, and I want to thank each of you for being here today. My first priority is to ensure the privacy and security of American families. Also making sure we have an environment where businesses can thrive. Right now, our Nation is facing threats from all across the world. We have adversaries like the Communist Party of China that continue to steal our data and technology, and force companies in China to turn over any user data their government wants.

Chinese backed companies like Huawei will hand over any sensitive data, including medical records, financial information, and social media accounts if they gain access to our markets. My colleague, Senator Cotton, introduced a bill which I support that would permanently prohibit the U.S. from sharing intelligence with countries that give Huawei access to their 5G networks. We have to do everything we can to provide Americans their information—protect Americans' information and our National Security. Mr. Phillips, what enforcement or what enforcement measures and oversight should be in place to ensure companies operate in the United States with access to personal and personal identifying information, disclose to the user where the company is housing the data?

Mr. PHILLIPS. Thank you, Senator Scott, for your question. To my mind, it is a question about materiality, what matters to those consumers. And I do think it is very well within Congress's purview to consider that question and to legislate upon it. I think increasingly, as we live in a globalized world, these kinds of questions where the data are, are important questions. But it is important to note that China has data localization.

And it is very important, as we have all been discussing, for the liberal democracies of the world that have a more open approach to Internet governance to find a path forward together.

Senator SCOTT. Thank you. When entering international privacy agreements, how do we ensure the U.S. places Americans' privacy interests first? Mr. Phillips.

Mr. PHILLIPS. Thank you, Senator. We don't, at the FTC, negotiate the privacy agreements. What we do is provide, in my view, a very important backstop. And that is when companies make commitments that they are participating in those agreements, make commitments about what they do as part of those agreements where they violate the law, where they make statements that aren't true that matter to consumers, we can bring enforcement actions against them. And that is what we have done for years.

Senator SCOTT. So what do you think about requiring online retailers to disclose more information like where data is housed or where products are produced?

Mr. PHILLIPS. I would have to give a little bit more thought to whether and to what extent that is material to consumers. I do think over time that is an increasing concern and it is definitely something within Congress's purview.

Senator SCOTT. I can't imagine why we don't know where Amazon and Wal-Mart don't tell U.S. where products are made, where services are provided, or where apps are created. So what do you think is the biggest safeguard that should be put in place to protect our data better?

Mr. PHILLIPS. Well, I think we have all been talking about for purposes of Americans and their privacy, a privacy bill. The difficulty we are facing today is in part or in large part to do with the European courts visa VR practices, not on the consumer side, but on the National Security side. And I do think as we have these discussions moving forward, as I said in my testimony, we do want to understand and defend American values, and we don't want our security not to be an important part of that conversation.

Mr. PHILLIPS. Thank you. Thank you, Mr. Chairman.

The CHAIRMAN. Thank you very much. This has been a very, very informative hearing, and some very talented and knowledgeable witnesses. I thank all five of you. And at this point we will close the hearing. Oh, Senator Rosen.

STATEMENT OF HON. JACKY ROSEN,
U.S. SENATOR FROM NEVADA

Senator ROSEN. Senator Rosen. Yes, I am here and I know I am always the last one, but I am waiting. I am here.

The CHAIRMAN. Well, why don't we recognize you for 5 minutes then?

Senator ROSEN. Well, thank you, my friend. I appreciate it. And I appreciate this hearing. It has been really informative. And I want to talk about the importance of small business, of course. So Nevada is home to more than a quarter of a million small businesses. Small businesses are the driving force that powers my state's economic engine. But unfortunately, this pandemic has dealt business owners unprecedented challenges and obstacles. We need to be doing all we can to ensure that our small and medium-sized businesses can survive this pandemic and receive the resources and support they need to compete both domestically and internationally. Nevada based companies that conduct business outside the

U.S. depend on agreed upon frameworks that ensure they are adhering to their international client's home country rules and regulations, including those related to data protection and security.

So actually, there are over 30 companies in Nevada that depended on the now invalidated Privacy Shield. The framework, of course, that allows for the transferring, processing, and storing of personal data from the EU to the U.S. Businesses such as game development firm Play Studios, and software company Action Verb that are headquartered right in Las Vegas. So unfortunately, it is quite small size and medium-sized businesses that have had the most to lose if the EU and the U.S. aren't able to reach a new agreement.

Larger businesses with large compliance departments, they will really have the upper hand, and it gives them a big competitive edge over the smaller firms, not just in Nevada but across the country. So to both Ms. Espinel and Mr. Sullivan, before the adoption of Privacy Shield, there was a different mechanism that enabled personal data transfers from the U.S. to the EU until it was also invalidated by European court in 2015. With that in mind, as we look to a new Administration and future talks with our EU partners, what issues do we as policymakers need to address to deal with the underlying intelligence gathering concerns that have plagued these frameworks so we just don't end up in the same place over and over again?

Mr. SULLIVAN. Thank you, Senator, for your question. Just to reiterate, maybe add a few more details to your point on SMEs, I want to make sure everyone has a sense of just how cost effective Privacy Shield is. And as you noted, its predecessor's framework, Safe Harbor was. Right now, the fees or the fees at least up until *Schrems II* for participation in the program, are based on your annual revenue.

So if you were a company with annual revenue of up to $5 million, your certification and participation in Privacy Shield, the fee you paid was $250. If you were $5 million to $25 million, it was $650. I won't run you through the whole list, but if you are over $5 billion in annual revenue, what you paid for Privacy Shield was $3,250. It was again by far the most cost effective approach for transatlantic data transfer mechanisms. And that is why—it is just another element as to why we think it is so critical, particularly for SMEs.

The other thing I want to make folks aware of, our Privacy Shield team and our other teams, our global data policy team, engage in regular roadshows and they meet—they have a particular remit and focus on SMEs to make sure they understand, you know, if they do want to go global, if they do want to do business in Europe, how do they do that? What are the issues? What are the options? Another thing, again, at the risk of being redundant, because we don't have a global standard on data protection privacy, because countries do take different approaches, we also have another mechanism in place. You know, we have come up, because it is going to take a while for a global standard, we have got to bridge our differences.

And so we had Privacy Shield with Europe. We had Safe Harbor before that, as you just noted. We also in APAC have something

called the Cross-Border Privacy Rules System. And again, that is another way that we can bridge our differences with some common baseline standards around privacy. And so, again, we do a lot on the APAC's CBPR system to make sure that companies, particularly SMEs, understand that that is an option that is available to them.

All of this is to promote interoperability so that companies are facing, again, increasingly fragmented and unaligned regulatory regimes around the world on these issues, and SMEs in particular, cannot pay the costs on this. And so we have got to come up with these structures until we get to a time where there is a single global standard.

Without sounding like I am criticizing GDPR, I do think it is important to note, when it went into effect in May 2018, what happened was you saw the big multinationals actually expand their market share and thousands of U.S. SMEs basically made the determination that it was either too expensive to comply with GDPR, or that the potential fines were simply too onerous and they withdrew from the market.

And so we spent a lot of time and effort to make sure that we are ensuring market access for SMEs. Hopefully, I answered your question. If not, I am happy to follow up if I missed something. Thank you.

Senator ROSEN. No, that is fine. I know my time has expired, but——

Ms. ESPINEL. Chairman Wicker, would I be able to respond Senator Rosen's question?

The CHAIRMAN. Yes, please.

Senator ROSEN. Thank you.

Ms. ESPINEL. Thank you. Senator Rosen, first, I want to note that not only is Nevada home to many small businesses, but as you know, in the jobs report, the latest jobs report we put out, Nevada was the number one highest growth rate for software jobs in the country. So I want to congratulate you for that and the work that you are doing on STEM training is going to create jobs across the country. In terms of the issue at hand, there are three things that I think we need to do. The first is we need to negotiate an enhanced U.S.-EU privacy agreement. We have talked a lot about that. I commend Jim Sullivan for the work that he and his team are doing.

Two, long term we need to reach a consensus with a group of democracies that share our values on intelligence gathering. And I think that will be a real challenge and an opportunity for U.S. leadership as we move forward. And third, we need to rebuild our foreign alliances and we need to make trust the basis of those.

And I think that both underpins and is overarching the first two. That those three elements, the urgent need for enhanced U.S.-EU Privacy Shield, a long-term solution on appropriate safeguards on intelligence norms, and then rebuilding our foreign alliances with the trust underlying them that they warrant, are critical to moving forward.

Senator ROSEN. Thank you very much for both of those answers. I look forward to working with you on finding the best ways that we can support all those tech jobs that keep growing in Nevada

and, of course, all the small and medium sized businesses that do want to expand across the Nation. Thank you, Mr. Chairman, for indulging my time.

The CHAIRMAN. Thank you. Thank you, Senator Rosen. You and I need to vote, and we will now close this hearing. The hearing record will remain open for two weeks. During this time, Senators are asked to submit any questions for the record. Upon receipt, the witnesses are requested to submit their written answers to the Committee as soon as possible. Thank you. We conclude the hearing, and we very much appreciate your participation.

[Whereupon, at 11:51 a.m., the hearing was adjourned.]

A P P E N D I X

AMERICAN CIVIL LIBERTIES UNION
Washington, DC, December 9, 2020

Hon. ROGER WICKER,
Chairman,
Committee on Commerce, Science, and Transportation,
U.S. Senate,
Washington, DC.

Hon. MARIA CANTWELL,
Ranking Member,
Committee on Commerce, Science, and Transportation,
U.S. Senate,
Washington, DC.

RE: The Invalidation of the EU-US Privacy Shield and the Future of Transatlantic Data Flows

Dear Chairman Wicker, Ranking Member Cantwell, and Members of the Committee,

On behalf of the American Civil Liberties Union ("ACLU"),[1] we submit this letter for the record in connection with the Senate Commerce Committee's hearing, "The Invalidation of the E.U.-U.S. Privacy Shield and the Future of Transatlantic Data Flows." We write to address the legal reforms that must be made to permit the free flow of data from the E.U. to the U.S., in the wake of the *Schrems II* decision by the Court of Justice of the European Union ("CJEU"), and subsequent guidance by the European Data Protection Board. These changes are essential to ensure that small and large businesses alike will not continue to suffer financial consequences through no fault of their own.

The reforms discussed below would also provide essential privacy protections for Americans, whose communications and data are swept up by the U.S. government's foreign intelligence surveillance in enormous quantities.[2] As technological advances permit ever-broader forms of surveillance—including bulk collection—there is an urgent need for stronger legal safeguards.

On July 16, the CJEU struck down the E.U.-U.S. Privacy Shield, used by over 5,300 companies, for failing to provide a sufficient level of protection for E.U. data.[3] Specifically, the court found that U.S. surveillance authorities, including Section 702 of the Foreign Intelligence Surveillance Act ("FISA") and Executive Order ("EO") 12333, permit large-scale surveillance that is not strictly necessary to the needs of

---

[1] For nearly 100 years, the ACLU has been our nation's guardian of liberty, working in courts, legislatures, and communities to defend and preserve the individual rights and liberties that the Constitution and the laws of the United States guarantee everyone in this country. The ACLU takes up the toughest civil liberties cases and issues to defend all people from government abuse and overreach. With approximately two million members, activists, and supporters, the ACLU is a nationwide organization that fights tirelessly in all 50 states, Puerto Rico, and Washington, D.C., for the principle that every individual's rights must be protected equally under the law, regardless of race, religion, gender, sexual orientation, disability, or national origin.

[2] *See, e.g.,* Barton Gellman *et al., In NSA-Intercepted Data, Those Not Targeted Far Outnumber the Foreigners Who Are,* Wash. Post (July 5, 2014), *https://www.washingtonpost.com/world/national-security/in-nsa-intercepted-data-those-not-targeted-far-outnumber-the-foreigners-who-are/2014/07/05/8139adf8-045a-11e4-8572-4b1b969b6322—story.html;* John Napier Tye, *Meet Executive Order 12333: The Reagan Rule that lets the NSA spy on Americans,* Wash. Post (July 18, 2014), *https://www.washingtonpost.com/opinions/meet-executive-order-12333-the-reagan-rule-that-lets-the-nsa-spy-on-americans/2014/07/18/93d2ac22-0b93-11e4-b8e5-d0de80767fc2—story.html.*

[3] C-311/18, *Data Protection Comm'r v. Facebook Ireland Ltd. & Maximilian Schrems "Schrems II")* (July 16, 2020), *http://curia.europa.eu/juris/document/document.jsf?text=&docid=228677&pageIndex=0&doclang=EN&mode=req&dir=&occ=first&part=1&cid=15476758.*

the state. The court also found that the Privacy Shield failed to create adequate redress mechanisms for Europeans whose data is transferred to the U.S.—namely, the ability to be heard by an independent and impartial court.

In addition to invalidating Privacy Shield, the CJEU's ruling indicated serious problems with companies' reliance on a separate mechanism, Standard Contractual Clauses (SCCs), for data transfers from the E.U. to the U.S., given the scope of U.S. surveillance and obstacles to redress. Based on the CJEU's ruling, the European Data Protection Board recently issued draft guidance concerning SCCs that would make it virtually impossible to transfer personal data to "electronic communication service providers," 50 U.S.C. §1881(b)(4), inside the U.S. for processing.[4] Indeed, the Irish Data Protection Commissioner has already issued a preliminary order to Facebook to halt its transfers to the U.S. about its E.U. users.[5]

The CJEU's ruling and the European Data Protection Board's guidance pose significant problems for U.S. companies in places as diverse as Boca Raton, Florida, San Francisco, California, and Cleveland, Ohio, who relied on Privacy Shield and currently rely on SCCs to transfer data from the E.U. for processing and storage in the U.S. In many cases, companies rely on these data-transfer mechanisms for critical functions, such as providing services to customers overseas or human resources to a global workforce.

Below, we describe several reforms critical to ensuring future transatlantic data flows. Although we propose reforms to both Section 702 and EO 12333 surveillance, the Section 702 reforms are especially urgent. That is because the Section 702 collection of data "at rest" inside the United States is an insurmountable obstacle to the functioning of SCCs.

In particular, to address the CJEU's ruling, Congress must:

- Narrow the scope of Section 702 and EO 12333 surveillance;
- Expand the role of the Foreign Intelligence Surveillance Court in Supervising Section 702 and EO 12333 surveillance;
- Ensure that individuals affected by U.S. surveillance can challenge improper surveillance in court; and
- Limit retention and use of information under Section 702 and EO 12333.[6]

Separately, Congress must also work to pass comprehensive consumer privacy protections. That legislation must provide clear and strong data-usage rules and ensure that discrimination cannot take on new life in the 21st century. It must also allow states to enact stronger protections and provide people the opportunity to sue companies that violate their privacy. However, we note that these privacy protections, while essential, will not address the concerns of the CJEU, which focused on the U.S. government's overbroad surveillance authorities and obstacles to redress for government surveillance. To address the ruling in *Schrems II,* the path forward requires reforms to Section 702 and EO 12333.

BACKGROUND

Under E.U. law, companies are generally forbidden from transferring personal data to non-E.U. countries on a repeated or systematic basis, unless the transfer is conducted pursuant to one of the following:

> *1. Special Transfer Mechanisms.* Companies may, through contracts such as SCCs or similar mechanisms, establish certain rules for data transfers to safeguard privacy rights. In some contexts, these safeguards can compensate for deficiencies in a non-E.U. country's law—*e.g.,* if the non-E.U. country lacks protections for consumer privacy, companies may use an SCC to commit to extend basic rights to consumers vis-à-vis the companies.
>
> In the U.S., however, no contract is capable of overcoming the fundamental problems with U.S. law identified by the CJEU: namely, the scope of U.S. foreign intelligence surveillance and obstacles to redress. No contract between two

---

[4] *See* European Data Protection Board, *Recommendations 01/2020 on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data* (Nov. 10, 2020), *https://edpb.europa.eu/sites/edpb/files/consultation/edpb—recommendations—202001—supplementary measurestransferstools—en.pdf; see also, e.g.,* Omer Tene, Vice President at the International Association of Privacy Professionals, *Quick Reaction to EDPB Schrems II Guidance, https://www.linkedin.com/pulse/quick-reaction-edpb-schrems-ii-guidance-omer-tene* ("it's hard to see a clear path for data transfers to the US").

[5] Sam Schechner & Emily Glazer, *Ireland to Order Facebook to Stop Sending User Data to U.S.,* Wall St. J. (Sept. 9, 2020), *https://www.wsj.com/articles/ireland-to-order-facebook-to-stop-sending-user-data-to-u-s-11599671980.*

[6] These reforms would not necessarily be sufficient to satisfy U.S. constitutional requirements.

companies can narrow the sweep of government surveillance or ensure that targeted customers receive notice of classified surveillance.

2. Adequacy Decision. The European Commission may conclude, as a categorical matter, that a non-E.U. country provides an "adequate" level of protection through its domestic law and international commitments—as it did through Safe Harbor and then Privacy Shield—but the Commission's adequacy decisions are subject to review by the CJEU. The CJEU has interpreted the "adequacy" standard to require that the non-E.U. country provide a level of protection of fundamental rights and freedoms that is "essentially equivalent" to those provided under E.U. law.[7]

Because the CJEU has identified fundamental defects in U.S. law, discussed in greater detail below, U.S. reforms should be a prerequisite to the negotiation of a new E.U.-U.S. data-transfer agreement. Indeed, European Commissioner Didier Reynders has stated publicly that "no quick fix" will adequately address the requirements of E.U. law.

But even if the European Commission were to agree to a quick fix, U.S. companies would still face substantial economic risks—including the risk that individual member-state Data Protection Authorities ("DPAs") would halt data flows. In analyzing transfers conducted pursuant to SCCs and similar mechanisms, DPAs are not bound by the European Commission's conclusions about whether a non-E.U. country's laws are adequate. Indeed, prior Commission adequacy decisions have acknowledged DPAs' authority to arrive at their own independent conclusions about whether to halt data transfers. And notably, in *Schrems II,* the CJEU held that DPAs are required to suspend data transfers if they conclude that such transfers are unlawful.

To ensure that any new E.U.-U.S. data-transfer agreement withstands CJEU scrutiny, and to ensure that U.S. companies do not pay the price for a failed "quick fix," Congress must enact the reforms below.

REFORMS TO U.S. LAW

1. Narrow the Scope of Section 702 and EO 12333 Surveillance

For an adequacy decision to survive CJEU scrutiny, the non-E.U. country's laws may interfere with the protection of personal data "only in so far as is strictly necessary."[8] In *Schrems I,* the CJEU explained that, in conducting surveillance, the third country must employ an "objective criterion" limiting surveillance to purposes that are "specific, strictly restricted and capable of justifying the interference."[9] It also held that government access "on a generalised basis to the content of electronic communications" violates the "essence" of the right to private life.[10] In *Schrems II,* the CJEU elaborated on these concerns with respect to Section 702 and EO 12333 surveillance. It explained that Section 702 "does not indicate any limitations on the power it confers to implement surveillance programs," and it observed that the U.S. government collects communications in "bulk" under EO 12333[11]—*i.e.,* it accesses communications on a "generalised basis."

Congress should act immediately to narrow the scope of both Section 702 and EO 12333.

With respect to Section 702, Congress can begin to address this issue by requiring an executive branch finding of reasonable suspicion that surveillance targets are "foreign powers" or "agents of a foreign power" outside of the United States—a clear "objective criterion" to justify the interference with private communications.[12] In the alternative, Congress could narrow the definition of "foreign intelligence information" under 50 U.S.C. ?1801(e), though this reform may not be sufficient to address the CJEU's concerns about the breadth of Section 702 surveillance.

With respect to EO 12333, Congress should prohibit bulk collection and require that surveillance be directed at specified targets. Separately, Congress should narrow EO 12333's definition of "foreign intelligence," which currently allows the gov-

---

[7] *Schrems II* ¶¶ 201, 203.

[8] C-362-14, *Schrems v. Data Protection Comm'r ("Schrems I")* ¶ 92 (Sept. 23, 2015), *http://curia.europa.eu/juris/document/document.jsf?text=&docid=169195&pageIndex=0&doclang=en&mode=lst&dir=&occ=first&part=1&cid=10588011.*

[9] *Schrems I* ¶ 93.

[10] *Schrems I* ¶ 94.

[11] *Schrems II* ¶ 183.

[12] Notably, "foreign power" and "agent of a foreign power" are defined rather broadly under FISA to include international terrorists, political factions, and entities acting under a foreign government's effective control. See 50 U.S.C. § 1801(a)-(b).

ernment to conduct surveillance to obtain any "information relating to the capabilities, intentions, or activities of . . . foreign persons."

2. Expand the Role of the Foreign Intelligence Surveillance Court in Supervising Section 702 and EO 12333 Surveillance

In invalidating Privacy Shield, the CJEU focused largely on the lack of independent approval of surveillance targets under Section 702 and EO 12333. Under Section 702, the role of the FISC consists mainly of an annual review of general targeting and minimization procedures; the FISC does not evaluate whether there is sufficient justification to conduct surveillance on specific targets. Under EO 12333, the FISC has no role at all.

To address these concerns, and to ensure greater protection for Americans whose communications and data are swept up in this surveillance, Congress must enact significant changes to the FISC's role in supervising Section 702 and EO 12333 surveillance. At a minimum, the FISC or other independent entity should review targeting decisions on an individual ex post basis. Although this reform would likely require Congress to expand the number of FISC judges, it would enhance privacy protections for Americans swept up in this surveillance and, given the concerns of the CJEU, it is essential to ensuring the free flow of data between the E.U. and the U.S.

3. Ensure that Individuals Affected by U.S. Surveillance Can Challenge Improper Surveillance in Court

In *Schrems II,* the CJEU affirmed that individuals whose personal data is transferred from the E.U. must have access to judicial remedies to challenge the treatment of their data—remedies they lack under the current legal framework in the U.S. As a general matter, individuals do not receive notice that their information has been collected for foreign intelligence purposes, even in cases where notice would not jeopardize an active investigation. The lack of notice makes it difficult—if not impossible—for people subjected to illegal surveillance to establish standing to challenge that surveillance in U.S. courts.

Congress should enact two key reforms to expand access to meaningful remedies.

First, a "standing fix": Congress can and should pass legislation to more clearly define what constitutes an "injury" in cases challenging government surveillance, as Senator Wyden and others proposed in a 2017 reform bill. While standing is a constitutional requirement, the Supreme Court has been clear that Congress has a role to play in defining what qualifies as an "injury" for the purposes of standing. Congress could, for example, explain that where a person takes objectively reasonable protective measures in response to a good-faith belief that she is subject to surveillance, those protective measures constitute an injury-in-fact. This reform would allow more individuals to begin to litigate claims of unlawful surveillance in the public courts.

Second, Congress should require the executive branch to provide delayed notice of foreign intelligence surveillance to targets of that surveillance, where such notice would not result in an imminent threat to safety or jeopardize an active investigation. In addition, FISA should be modified to define "derived," to ensure that the government fully complies with its existing statutory notice obligations.

4. Limit Retention and Use of Information Under Section 702 and EO 12333

In *Schrems II,* the CJEU found that U.S. surveillance law lacked sufficient safeguards, including with regard to the access and use of information.[13] Under Section 702, the government has broad authority to retain and use the data it has collected. It can retain communications indefinitely if they are encrypted or are found to contain foreign intelligence information. Even for data that does not fall into either of these categories, the default retention period is as long as five years. The retention limitations for communications and data collected under EO 12333 are similar.

Congress should enact additional restrictions on the use and retention of data collected under Section 702 and EO 12333. In particular, Congress should require that where an agency seeks to retain data beyond the default retention period, the agency must establish that the data falls within a narrow subset of critical "foreign intelligence." Congress should also limit the Section 702 and EO 12333 default retention period to three years.

---

[13] *Schrems II* ¶ 180.

CONCLUSION

For more information, please contact Senior Legislative Counsel Kate Ruane at *kruane@aclu.org* or (202) 675-2336, or Senior Staff Attorney Ashley Gorski at *agorski@aclu.org* or (212) 284-7305.

Sincerely,

RONALD NEWMAN,
National Political Director,
National Political Advocacy Department.

KATHLEEN RUANE,
Senior Legislative Counsel,
National Political Advocacy Department.

ASHLEY GORSKI,
Senior Staff Attorney,
National Security Project.

cc: Members of the Senate Committee on Commerce, Science, and Transportation

---

RESPONSE TO WRITTEN QUESTIONS SUBMITTED BY HON. AMY KLOBUCHAR TO HON. NOAH JOSHUA PHILLIPS

Senator Klobuchar: *Economic Impact of the Privacy Shield Invalidation on Small Business.* More than 5,300 U.S. companies—which contribute nearly $1.1 trillion in total U.S. trade in goods and services with the EU—were impacted by the invalidation of the Privacy Shield. In your testimony, you highlight that more than 65 percent of small and medium-sized businesses participated in the Privacy Shield and that almost two-thirds of worldwide startups surveyed had customers or users in other countries.

Question 1. Can you elaborate on your concerns regarding the impact of the Privacy Shield's invalidation on small and medium-sized companies?

Answer. My concern is that the invalidation of Privacy Shield will have an outsized impact on small and medium-sized businesses. The program allowed U.S. businesses interested in European markets a simple and economical way to engage in necessary data transfers, for example of payment and shipping information. That is why some 65 percent of the thousands of companies that enrolled in Privacy Shield were small and medium-sized businesses. Without it, these firms may be forced to shut down or limit access to transatlantic markets. While there are other legal bases through which to transfer the data of European customers to the U.S., they are costly and complicated; in most cases they are not viable options for smaller business. The net effect will be higher costs for small and medium-sized businesses and an uneven playing field that favors larger firms.

Question 2. In your view, what measures help ensure secure and stable cross-border data protections, particularly for small and medium-sized businesses?

Answer. Small and medium-sized businesses, like all businesses, benefit from stable, efficient, and economical means to transfer data across borders. The most important thing we can do is to finalize a new agreement with our European partners that will once again permit U.S. businesses efficiently and economically to transfer data from Europe. U.S. and EU negotiators are already hard at work on a replacement for Privacy Shield, and the Biden Administration should make it a priority to complete that effort.

Congress should continue to support these efforts, as should the Federal Trade Commission.

As we move forward, in particular in engagement with our allies in Europe, we must ensure that an American voice and point of view is part of the discussion about Internet governance, and be willing to defend our approach. Liberal democracies that value free speech and privacy should prioritize regulatory interoperability, and not let relatively minor differences impede mutually-beneficial commerce.

RESPONSE TO WRITTEN QUESTIONS SUBMITTED BY HON. AMY KLOBUCHAR TO PROF. NEIL M. RICHARDS

Consumer Access and Control/Privacy Shield Invalidation. In July, the European Union struck down the Privacy Shield following allegations that Facebook was providing U.S. intelligence agencies with unlimited access to customers' data. In your testimony, you note that if the U.S. had "adequate" privacy legislation, the Privacy Shield would be unnecessary. Last December, I joined Senators Cantwell, Schatz, and Markey in introducing comprehensive privacy legislation to establish digital rules to protect consumers' data.

Question 1. While our bill is focused on commercial surveillance, do you agree that legislation like ours would help the U.S. strengthen privacy protections and rebuild trust with the EU?

Answer. Thank you for the opportunity to answer such perceptive and important questions. Strong, baseline commercial privacy legislation is essential to rebuilding trust with our EU trading partners and allies—and it would also be a tremendously good thing for Americans.

First, commercial privacy protections would strengthen our critically important relationships with the EU. At the December hearing, Mr. Sullivan from the Commerce Department suggested that there is not an international consensus on privacy rights. Simply put, he is wrong. There is an international consensus, and it is one being driven by the EU approach to privacy—including commercial privacy—as a fundamental right. As I have explored in some of my scholarship, while the United States used to be the global leader on privacy, it has ceded that right by inaction. The failure of successive Congresses over the past two decades to pass a comprehensive privacy statute has meant not just that Americans have had insufficient privacy protection in a time of rapid technological change, not just that this inadequacy has affected our global reputation, not just that the EU has taken the lead on global privacy standards, but that the EU standard has become a global trade standard. If the United States wants to participate in these vital markets, it now has to do so according to standards that the EU has shaped through instruments like the Data Protection Directive and the GDPR.[1]

It's important to stress that since the 1990s, the European data protection regime (first the Directive, and since 2018 the GDPR) has primarily focused on what we'd call commercial privacy. The EU originated as the Common Market and has evolved from a trade federation, under the sensible idea that countries that trade together and share common economic interests become stronger allies and better partners. Before the Snowden Revelations and the *Schrems* litigation that it spawned, issues of cross-border data flows were primarily commercial trade issues, and the issues of "adequacy" of U.S. law largely revolved around whether companies like Google were processing the data of Europeans in ways that were consistent with EU law and the fundamental right to privacy and data protection those laws protect. The *Schrems* litigation has been of course about intelligence services accessing the data of Europeans, but if the United States wants to be deemed "adequate" and participate in the international data trade as an equal, respected, trusted partner, robust commercial privacy protections for all personal data held by U.S. companies will be essential. In this way, as I suggested at the December hearing, comprehensive commercial privacy reform by this Congress is a necessary (though not sufficient) condition for preserving and building trusted, sustainable, and profitable commercial relationships with our key European allies around personal data.

Second, putting the relationships with our European friends entirely to the side, comprehensive privacy reform would be good for America. Today, American consumers are at the mercy of powerful corporations that collect and process their data. The current American privacy regime relying on fictional notice and illusory choice utterly fails to protect American consumers from manipulation and exposure to data breaches, and I am gratified to see that a bipartisan consensus has emerged that recognizes these facts and is keen to do something about them. The good news is that comprehensive privacy reform can be good for business as well as for consumers. Good businesses rest on trust, and the kinds of trusted, sustainable relationships that can last for decades. To use a technology example, many American consumers have decades-long trusted relationships with companies like Apple or Microsoft, and feel comfortable sharing sensitive information because they believe that those companies will be discreet, honest, protective, and loyal with their data. Unfortunately, this is not the case for many companies in the technology sector, particularly those who offer "free" services in exchange for *sotto voce* data barter trans-

[1] See Woodrow Hartzog & Neil M. Richards, *Privacy's Constitutional Moment and the Limits of Data Protection* 61 BOSTON COLLEGE LAW REVIEW 1687 (2020).

actions, the terms of which are almost impossible for consumers to understand, much less agree to freely. Sensible comprehensive privacy laws that protect consumers would reward the many companies that are already engaging in such behavior, and would eliminate any competitive advantage to cheat when it comes to data protection and consumer protection.

Question 2. Our bill also includes a provision to require companies to establish a privacy security program to regularly assess security vulnerabilities. Do you agree that data security programs can play a key role in ensuring secure and stable cross-border data protections?

Answer. Absolutely. Meaningful data security requirements that ensure corporate accountability are critical for the consumer trust that is necessary for cross-border data sharing. In addition, data security has long been an obvious and essential part of the language of data protection, and it is part of the requirements of the GDPR for adequate levels (or to put it another way "essentially equivalent" levels) of data protection. GDPR Art. 45 & Recital 104. Comprehensive data security programs of the sort advocated by the FTC foreground the importance of data security, while they also regularize and professionalize its practice in firms. The key to security programs, however, is accountability—security program requirements must have teeth that require substantively adequate security under the circumstances and cannot be reduced to safe harbors that relieve companies of liability if they maintain minimal measures or go through a mere process of compliance.

RESPONSE TO WRITTEN QUESTIONS SUBMITTED BY HON. KYRSTEN SINEMA TO PROF. NEIL M. RICHARDS

Small Businesses. Small businesses power Arizona's growing economy. We need to remove unnecessary burdens, and increase transparency and accessibility to support small businesses.

Question 1. How does the European Court of Justice's invalidation of the Privacy Shield framework harm small businesses that need to transfer data to or from Europe?

Answer. The European Court of Justice's invalidation of the Privacy Shield framework harms all American businesses and consumers, but many small businesses are likely to suffer particular harms. Those businesses that need to transfer data from Europe can no longer rely on the Privacy Shield to protect the transfer, and as small businesses they are unlikely to possess the resources to generate binding corporate rules. In the absence of an adequacy determination, this leaves only the model contracts, whose validity was called into question by the ECJ in *Schrems II.* Under current post-*Schrems II* guidance from the European Data Protection Board, companies seeking to use the model contracts need to engage in a case-by-case analysis to assess the sufficiency of data protections for such transfers outside the European Economic Area. This analysis requires companies to assess not just the transfer, but the risks the transfer faces in the context of the privacy and intelligence regimes governing the transfer. In essence, this requires companies to engage in a full *Schrems II*-style ongoing analysis for each kind of transfer—something that would be daunting for a huge company like Google or Amazon, and would be impossible for many small businesses to engage in. Thus, the harm faced by American small businesses is the imposition of a difficult, if not impossible regulatory burden should they wish to make transfers of EU personal data to the United States. This problem is caused by the mismatch between privacy and data protection regimes in the United States and the EU.

Question 2. While a long-term solution is crafted, how can Congress support small businesses that need to transfer data to or from Europe?

Answer. The best thing that Congress could do is to pass a comprehensive privacy statute with meaningful redress options for consumers, including a private right of action. The closer our American privacy regime gets to "essential equivalence" with the level of protection on the consumer side in the GDPR, the easier it will be to reach a durable, sustainable reconciliation with the EU. This is particularly the case because the *Schrems II* judgment left the model contractual clauses mechanism for cross-border transfer largely intact, subject to the caveat that European data exporters have to assess the risks of access in violation of EU data protection rights. To the extent that small business (and certainly particular kinds of small businesses) are less likely to have the kinds of data that the U.S. Intelligence Community might seek to access, this will be less of a problem for them. On the other hand, as I explained in the previous answer scope, difficulty, and expense of this analysis will be beyond the resources of many small businesses. However, a higher level of pri-

vacy protection for all data held in the U.S. (especially the data of Europeans) would tend to lower the temperature of the cross-border conflict with the EU, making it easier to reach long term solution—ideally adequacy.

Speaking of adequacy, I note that at the December hearing, Mr. Sullivan from the Commerce Department suggested that adequacy was difficult, even impossible, to achieve, citing the examples of (I believe) India and Brazil as being countries very different from the United States. Mr. Sullivan's explanation was misleading at best and disingenuous at worst, as he forgot to mention a country that has adequacy which is very similar to the United States: Canada. Canada has had adequacy since the days of the old Data Protection Directive. If Canada can achieve adequacy with its own comprehensive privacy law, PIPEDA, the United States can as well, and I have great optimism that the new administration will take a more nuanced and informed approach to privacy and data protection issues than the perspective Mr. Sullivan espoused at the hearing.

The other things that Congress can do is related to remedies to challenge unlawful surveillance. Practical and legal obstacles to the challenge of assertedly unlawful surveillance programs in the United States are significant, and are in my opinion a significant rule of law challenge. As I argued in a widely-cited 2013 law review article, it is a basic element of the rule of law that a democratic, self-governing people should have the right to know and consent to what is being done by their intelligence services in their name, and there should be appropriate legal means to challenge surveillance programs that are asserted to be illegal or unconstitutional, just as with other government programs.[2] To the extent that there are currently obstacles to relief, such obstacles are a major part of the problem with U.S. law that led to the invalidation of the Safe Harbor Agreement in *Schrems I* and the Privacy Shield in *Schrems II*. Indeed, much of my own testimony in that case dealt with the substantial obstacles to relief—including standing doctrine—that plaintiffs face in surveillance challenges. Here, too, Congress can help. As the ACLU explained in its Statement on the Record in this hearing,

Congress should enact two key reforms to expand access to meaningful remedies.

> First, a "standing fix": Congress can and should pass legislation to more clearly define what constitutes an "injury" in cases challenging government surveillance, as Senator Wyden and others proposed in a 2017 reform bill. While standing is a constitutional requirement, the Supreme Court has been clear that Congress has a role to play in defining what qualifies as an "injury" for the purposes of standing. Congress could, for example, explain that where a person takes objectively reasonable protective measures in response to a good faith belief that she is subject to surveillance, those protective measures constitute an injury-in-fact. This reform would allow more individuals to begin to litigate claims of unlawful surveillance in the public courts.
>
> Second, Congress should require the Executive Branch to provide delayed notice of foreign intelligence surveillance to targets of that surveillance, where such notice would not result in an imminent threat to safety or jeopardize an active investigation. In addition, FISA should be modified to define "derived," to ensure that the government fully complies with its existing statutory notice obligations.
>
> American Civil Liberties Union, Statement on the Record re: The Invalidation of the EU–US Privacy Shield and the Future of Transatlantic Data Flows, December 9, 2020, at 5, available at *https://www.aclu.org/sites/default/files/field_document/2020-12-8_aclu_statement_for_the_record_senate_commerce_committee_hearing_on_privacy_shield.pdf*.

In my opinion, the reforms proposed by the ACLU (particularly the first) would be an excellent place for Congress to start.

---

[2] *See* Neil M. Richards, *The Dangers of Surveillance,* 126 HARV. L. REV. 1934 (2013).

RESPONSE TO WRITTEN QUESTIONS SUBMITTED BY HON. BRIAN SCHATZ TO PROF. NEIL M. RICHARDS

In your testimony, you asserted that it would be an "important and necessary" step, as well as good for business, to include a duty of loyalty in American privacy law.

Question 1. How would including duty of loyalty in Federal privacy law help American businesses? What other laws and regulations have included the duties of loyalty and care?

Answer. A duty of loyalty would help American businesses by setting clear rules of the road with respect to what constitutes fair business practices in an economy seemingly fueled by the exploitation of personal data. At an earlier hearing on privacy reform last fall, Senator, I was struck by the truth and wisdom of your statement that ethical companies already know that being loyal to their customers is good business, and so a duty of loyalty is only a burden for companies who want to be disloyal. In a market economy like ours, incentives for disloyalty can be a massive problem. When there are no rules, anything goes, and well-meaning companies staffed by ethical professionals nonetheless feel the unyielding pressures of the market to match the tactics of those who cheat and act in disloyal ways. A duty of loyalty would level the playing field and create incentives for competition and business innovation in ways that make things better for human customers, rather than creating incentives for companies to manipulate those consumers.

To be sure, manipulation is a real risk here. In her excellent book *The Age of Surveillance Capitalism,* Harvard's Shoshana Zuboff explains how tech companies discovered that digital services create transactional metadata with many uses.[3] These companies first used the data to *improve* their services, making them more efficient (such as by refining their search engines or interfaces) in ways that made things better for everyone—the tech companies and their human customers. The second step though, allowed companies to use transactional and other data to anticipate or *predict* what consumers could want or how they could be more effectively marketed to or influenced through "personalization." Zuboff goes on to describe a third stage—the use of transactional data and the techniques of behavioral science to *manipulate* consumers and have them behave in ways that were optimal to the companies or their advertiser clients. The first of these stages—product *improvement* through data—is a good thing in which the incentives of consumers and companies align to want better products. The second, *prediction* (sometimes called "personalization") is problematic when it is used in ways that are not in the best interests of the consumers, and the third—outright *manipulation*—is almost always problematic. At present, many uses of data that fall in categories two and three are legal. What's more, because thin, opt-out consent is easy to manufacture in a digital environment, any mere opt-out regime would be insufficient to protect consumers.[4] A duty of loyalty requiring companies to act in the best interests of their vulnerable human customers would help solve these problems. It would ensure that category two cases use the benefits of personalization to advance the interests of consumers, rather than preying on their individual vulnerabilities and human cognitive limitations. And it would also eliminate problematic cases of outright manipulation in category three, in which a company can use information it knows about a consumer to get them to dance to its own tune.

Duties of loyalty are not a new idea. In fact, they have a long and proud tradition in Anglo-American law. Many duties of loyalty arise in the fiduciary context, in which there is a less sophisticated party who must trust another who possesses more power, wealth, or expertise. As Dr. Woodrow Hartzog and I explain in our detailed paper, "A Duty of Loyalty for Privacy Law," our law has imposed loyalty duties on a wide variety of relationships typified by power differentials, including the law of trustees, corporate officers, agents, guardians of wards, lawyers, doctors, financial advisors, and others.[5] This body of law is extensive, and it has ancient roots in our law. Imposing a duty of loyalty on a relationship is a significant step, but it is a time-honored and appropriate step where there is vulnerability. As we argue in our paper on loyalty, the current digital environment is characterized by vulnerability, in which human consumers and citizens trust their online experiences and well-being to powerful, sophisticated, and highly capitalized technology companies.

---

[3] SHOSHANA ZUBOFF, THE AGE OF SURVEILLANCE CAPITALISM (2019).

[4] Neil Richards & Woodrow Hartzog, *The Pathologies of Digital Consent,* 96 WASH. U.L. REV. 1461 (2019).

[5] Neil Richards & Woodrow Hartzog, *A Duty of Loyalty for Privacy Law,* at ms. 22–23. (draft article forthcoming 2021), available at *https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3642217.*

In so doing, they are exposed to risks of manipulation, malware, identity theft, misinformation, nudging, and radicalization, among others. Our thesis is simple: "a duty of loyalty framed in terms of the best interests of digital consumers should become a basic element of U.S. data privacy law. A duty of loyalty would compel loyal acts and also constrain conflicted, self-dealing behavior by companies. It would shift the default legal presumptions surrounding a number of common design and data processing practices. It would also act as an interpretive guide for government actors and data collectors to resolve ambiguities inherent in other privacy rules. A duty of loyalty, in effect, would enliven almost the entire patchwork of U.S. data privacy laws. And it would do it in a way that is consistent with U.S. free expression goals and other civil liberties."[6]

At the hearing, we heard testimony that the European Commission considers the privacy laws of only a couple of countries to be "adequate" for international data transfers.

Question 2. Would a comprehensive privacy law that includes a duty of loyalty, help the United States achieve "adequacy" by the European Commission for international data transfers?

Answer. In all, the EU has granted adequacy to twelve nations or jurisdictions—Andorra, Argentina, Canada, the Faroe Islands, Guernsey, Israel, the Isle of Man, Japan, Jersey, New Zealand, Switzerland, and Uruguay. In addition, advanced talks are in progress with both South Korea and the post-Brexit United Kingdom.[7] I should also note that I followed the discussion of adequacy by Mr. Sullivan at the hearing with great interest. It is correct that the EU made an adequacy determination for a group of countries, but the prospects for adequacy are hardly as bleak as Mr. Sullivan suggested. As I explained in my response to Sen. Sinema's questions, Mr. Sullivan omitted Canada from his examples of countries that have obtained adequacy, though I must assume that this was merely an oversight on his part. In fact, if we look at the countries that have achieved adequacy, many are like the United States in important respects, and many of them are post-industrial democracies with advanced technologies and a robust commitment to the rule of law. Moreover, as I have already mentioned, the fact that Canada has been deemed adequate for two decades suggests that if the United States were to do the things that are necessary for adequacy, the EU would be delighted to bring the United States into that group.

I would be happy to talk more about adequacy at a future hearing, but for now I can answer your question succinctly by saying the following. The EU evolved from a trade federation and common market, and its laws are largely related to those interests. Until the *Schrems* litigation, adequacy was seen as almost exclusively a question of commercial data—were the protections for personal data in a particular country "essentially equivalent" to those in the EU such that an adequacy determination was warranted? The *Schrems* cases raise questions of intelligence gathering and of intelligence reform if the United States wishes to participate fully in the trans-Atlantic data trade, but it still remains true that adequacy determinations require substantial commercial protections. Article 45 of the GDPR governs adequacy determinations, and provides that, in assessing the adequacy of a country's level of data protection, the European Commission must look at (a) its rule of law, respect for human rights (including privacy and data protection), and relevant laws governing government access to personal data, as well as whether there are "effective and enforceable data subject rights and effective administrative and judicial redress for the data subjects whose personal data are being transferred"; (b) the existence of agencies that supervise compliance with data protection rules, and (c) a country's international commitments on data protection issues. GDPR Recital 104 helpfully clarifies this standard as whether the country can "offer guarantees ensuring an adequate level of protection essentially equivalent to that ensured within the Union."

Thus, there are two key parts to an adequacy determination: (1) a comprehensive privacy law imposing affirmative duties on companies that process our data, and providing remedies for violations, and (2) surveillance reform. With respect to (1), it is my opinion that a robust comprehensive U.S. privacy law containing a duty of loyalty would offer the best pathway to satisfying element (1). A duty of loyalty would constrain companies from acting in self-interested ways with our data (and with the data of EU citizens), it would offer remedies for violations, and it would contribute to the overall robustness and commitment to the rule of law for data

[6] *Id.* at ms. 7.

[7] European Commission, Adequacy Decisions, visited Feb. 9, 2021, available at *https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/adequacy-decisions_en.*

processing in the United States. It would go a long way to providing the key "essential equivalence" with respect to commercial data that adequacy hinges on—particularly as the EU itself is considering a variant of a duty of loyalty as it continues to develop its own privacy laws.[8] Moreover, for the reasons I have given in these responses and elsewhere in my writings, I believe that a duty of loyalty for privacy law in the United States would also be excellent policy.

○

[8] See, *e.g.,* European Commission, Proposal for a Regulation on European Data Governance (Data Governance Act), Nov. 25 2020 (containing a duty, like a duty of loyalty, under which "Data sharing providers that intermediate the exchange of data between individuals as data holders and legal persons should, in addition, bear fiduciary duty towards the individuals, to ensure that they act in the best interest of the data holders."), available at *https://ec.europa.eu/digital-single-market/en/news/proposal-regulation-european-data-governance-data-governance-act.*