AUTHENTICATED
U.S. GOVERNMENT
INFORMATION
GPO

INTERNATIONAL DATA FLOWS: PROMOTING DIGITAL TRADE IN THE 21ST CENTURY

HEARING

BEFORE THE

SUBCOMMITTEE ON
COURTS, INTELLECTUAL PROPERTY,
AND THE INTERNET

OF THE

COMMITTEE ON THE JUDICIARY
HOUSE OF REPRESENTATIVES

ONE HUNDRED FOURTEENTH CONGRESS

FIRST SESSION

NOVEMBER 3, 2015

Serial No. 114–49

Printed for the use of the Committee on the Judiciary



Available via the World Wide Web: http://judiciary.house.gov

U.S. GOVERNMENT PUBLISHING OFFICE
97–419 PDF WASHINGTON : 2016

For sale by the Superintendent of Documents, U.S. Government Publishing Office
Internet: bookstore.gpo.gov Phone: toll free (866) 512–1800; DC area (202) 512–1800
Fax: (202) 512–2104 Mail: Stop IDCC, Washington, DC 20402–0001

COMMITTEE ON THE JUDICIARY

BOB GOODLATTE, Virginia, *Chairman*

F. JAMES SENSENBRENNER, JR., Wisconsin
LAMAR S. SMITH, Texas
STEVE CHABOT, Ohio
DARRELL E. ISSA, California
J. RANDY FORBES, Virginia
STEVE KING, Iowa
TRENT FRANKS, Arizona
LOUIE GOHMERT, Texas
JIM JORDAN, Ohio
TED POE, Texas
JASON CHAFFETZ, Utah
TOM MARINO, Pennsylvania
TREY GOWDY, South Carolina
RAÚL LABRADOR, Idaho
BLAKE FARENTHOLD, Texas
DOUG COLLINS, Georgia
RON DeSANTIS, Florida
MIMI WALTERS, California
KEN BUCK, Colorado
JOHN RATCLIFFE, Texas
DAVE TROTT, Michigan
MIKE BISHOP, Michigan

JOHN CONYERS, JR., Michigan
JERROLD NADLER, New York
ZOE LOFGREN, California
SHEILA JACKSON LEE, Texas
STEVE COHEN, Tennessee
HENRY C. "HANK" JOHNSON, JR., Georgia
PEDRO R. PIERLUISI, Puerto Rico
JUDY CHU, California
TED DEUTCH, Florida
LUIS V. GUTIERREZ, Illinois
KAREN BASS, California
CEDRIC RICHMOND, Louisiana
SUZAN DelBENE, Washington
HAKEEM JEFFRIES, New York
DAVID N. CICILLINE, Rhode Island
SCOTT PETERS, California

SHELLEY HUSBAND, *Chief of Staff & General Counsel*
PERRY APELBAUM, *Minority Staff Director & Chief Counsel*

SUBCOMMITTEE ON COURTS, INTELLECTUAL PROPERTY, AND THE INTERNET

DARRELL E. ISSA, California, *Chairman*
DOUG COLLINS, Georgia, *Vice-Chairman*

F. JAMES SENSENBRENNER, JR., Wisconsin
LAMAR S. SMITH, Texas
STEVE CHABOT, Ohio
J. RANDY FORBES, Virginia
TRENT FRANKS, Arizona
JIM JORDAN, Ohio
TED POE, Texas
JASON CHAFFETZ, Utah
TOM MARINO, Pennsylvania
BLAKE FARENTHOLD, Texas
RON DeSANTIS, Florida
MIMI WALTERS, California

JERROLD NADLER, New York
JUDY CHU, California
TED DEUTCH, Florida
KAREN BASS, California
CEDRIC RICHMOND, Louisiana
SUZAN DelBENE, Washington
HAKEEM JEFFRIES, New York
DAVID N. CICILLINE, Rhode Island
SCOTT PETERS, California
ZOE LOFGREN, California
STEVE COHEN, Tennessee
HENRY C. "HANK" JOHNSON, JR., Georgia

JOE KEELEY, *Chief Counsel*
JASON EVERETT, *Minority Counsel*

CONTENTS

NOVEMBER 3, 2015

Page

OPENING STATEMENTS

The Honorable Darrell E. Issa, a Representative in Congress from the State of California, and Chairman, Subcommittee on Courts, Intellectual Property, and the Internet 1
The Honorable Jerrold Nadler, a Representative in Congress from the State of New York, and Ranking Member, Subcommittee on Courts, Intellectual Property, and the Internet 3
The Honorable Bob Goodlatte, a Representative in Congress from the State of Virginia, and Chairman, Committee on the Judiciary 4
The Honorable John Conyers, Jr., a Representative in Congress from the State of Michigan, and Ranking Member, Committee on the Judiciary 5

WITNESSES

Ambassador Peter Allgeier, President, Coalition of Service Industries (CSI)
Oral Testimony 12
Prepared Statement 15
Robert D. Atkinson, Ph.D., Founder and President, The Information Technology and Innovation Foundation
Oral Testimony 22
Prepared Statement 24
Victoria Espinel, President and CEO, BSA | The Software Alliance
Oral Testimony 46
Prepared Statement 48
Ed Black, President & CEO, The Computer & Communications Industry Association
Oral Testimony 54
Prepared Statement 56
Mark MacCarthy, Senior Vice President, Public Policy, Software & Information Industry Association
Oral Testimony 73
Prepared Statement 75

LETTERS, STATEMENTS, ETC., SUBMITTED FOR THE HEARING

Material submitted by the Honorable John Conyers, Jr., a Representative in Congress from the State of Michigan, and Ranking Member, Committee on the Judiciary 8

APPENDIX

MATERIAL SUBMITTED FOR THE HEARING RECORD

Prepared Statement of Edward M. Dean, Deputy Assistant Secretary for Services, International Trade Administration, U.S. Department of Commerce 120
Prepared Statement of Nuala O'Connor, President and CEO, Center for Democracy & Technology; and Gregory T. Jojeim, Director, Freedom, Security & Technology Project, Center for Democracy & Technology 124
Letter from Michael Beckerman, President & CEO, The Internet Association . 130

Page

Letter from Daphne Keller, Director of Intermediary Liability, Center for Internet and Society, Stanford Law School 133
Response to Questions for the Record from Ambassador Peter Allgeier, President, Coalition of Service Industries (CSI) 137
Response to Questions for the Record from Robert D. Atkinson, Ph.D., Founder and President, The Information Technology and Innovation Foundation .. 139
Response to Questions for the Record from Victoria Espinel, President and CEO, BSA | The Software Alliance 140
Response to Questions for the Record from Ed Black, President & CEO, The Computer & Communications Industry Association 142
Response to Questions for the Record from Mark MacCarthy, Senior Vice President, Public Policy, Software & Information Industry Association 146

INTERNATIONAL DATA FLOWS: PROMOTING DIGITAL TRADE IN THE 21ST CENTURY

TUESDAY, NOVEMBER 3, 2015

HOUSE OF REPRESENTATIVES

SUBCOMMITTEE ON COURTS, INTELLECTUAL PROPERTY, AND THE INTERNET

COMMITTEE ON THE JUDICIARY

Washington, DC.

The Subcommittee met, pursuant to call, at 1 p.m., in room 2141, Rayburn House Office Building, the Honorable Darrell E. Issa (Chairman of the Subcommittee) presiding.

Present: Representatives Issa, Goodlatte, Collins, Smith, Chabot, Jordan, Poe, Marino, DeSantis, Nadler, Conyers, Chu, DelBene, Jeffries, Cicilline, Peters, Lofgren, and Johnson.

Staff Present: (Majority) Vishal Amin, Senior Counsel; Eric Bagwell, Clerk; and (Minority) Jason Everett, Minority Counsel.

Mr. ISSA. The Committee will come to order.

Today's hearing concerns digital trade, and specifically cross-border data flows. The modern economy requires data flow and to flow freely.

Individuals and businesses rely on technology and the efficient and reliable movement of data across borders. The recent decision by the European Court of Justice, invalidating the 15-year-old Safe Harbor Agreement between the United States and the European Union, created uncertainty that's bad for business everywhere. We hear that a new Safe Harbor Agreement is imminent. But if an agreement is not reached by the end of January 2016, then the consequences for transatlantic data flow and business operations could be dire.

To help us reach a new agreement with the EU, the House passed a Judicial Redress Act last month. Though it still awaits Senate action, it is a strong move by the House to support—in support of reaching this vital agreement.

But cross-border data flow are not simply a transatlantic issue. They also figure prominently in the Trans-Pacific Partner Agreement, or TPP. As we consider digital trade issues more globally, it is important to view the tactics being used to restrict it as much as any other point of it. The trade barriers being used to restrict cross-border data flows are simply nontariff trade barriers. By any other name, it is protectionism, and it hurts U.S. competitiveness; it hurts the very countries who are implementing these protec-

tionist agreements, and ultimately, it will hurt global trading with all the partners who depend on data free flow in a 21st Century.

These trade barriers include localization requirements for cloud computing. That means that instead of harnessing the economies of scale that come from a cloud, companies will be forced to house in facilities in individual countries, resulting in duplicative infrastructure and higher costs. Let us bear in mind that a location anywhere on the face of the earth is a location everywhere on the face of the earth. And many countries seem to ignore that in favor of basically an infrastructure construction project being mandated in their country.

And it's not just technology companies that can be harmed by these types of digital trade barriers. In the financial services industry, banks use a security practice known as charting, that splits a single customer's information into discreet packets that are stored in multiple locations to prevent a hacker from compromising it. By its very definition, this practice would be impossible without the free flow of data.

In July, we held a hearing on The Internet of Things, or IOT. This new era of technology relies on sensors transmitting data to a cloud for analysis. If the data cannot flow freely around the globe, then The Internet of Things technologies will not be as successful as they could be, and, in fact, could restrict many of the technologies already implemented in The Internet of Things.

If countries are allowed to unduly restrict data flow, what is to stop them from creating new market access requirements that require companies to share source code, trade secrets, utilize—utilize or source solely from local companies, and more absurdly, force U.S. studios to alter their story line of a movie as a condition of market access.

The last one isn't that absurd. A report published just last week by the U.S.-China Economic and Security Review Commission, explains just how China regulator—China's regulators do just that as a condition of market access.

As this Committee works to promote digital trade, we are continuing a long battle against market access barriers that take surprisingly, and oftentimes, strange forms.

Though the issues can oft-times seem complex, the goal here is to actually make this simple and understandable for the American people to ensure free and fair trade, improving U.S. competitiveness globally.

Digital trade helps drive the modern economy, and I look forward to our witnesses today and a healthy debate on these issues.

Last but not least, it goes without saying that no one owns data in a global environment exclusively. An economic transaction for an American who is traveling in a foreign country, requires a lookback to their country. If the United States refuses to provide that data, while another country refuses to provide the information as to what is being bought or what service is being procured, then, in fact, you have a standoff; I won't let my data flow to you to tell you what customer X is buying, and you won't tell me if customer X can pay for it. Can you imagine trying to travel with a MasterCard or a Visa or an American Express that simply couldn't

cross international lines? Sounds absurd? Not if everyone says, my data is mine, and I won't share.

And with that, I recognize the Ranking Member for his opening statement.

Mr. NADLER. Thank you, Mr. Chairman.

Today's global economy is largely a digital economy. Thanks to the Internet, massive amounts of data can be sent across the global in an instant, connecting businesses and consumers alike. The ability to easily transmit data at low cost throughout the world has spurred tremendous innovation and fostered significant economic growth. But various countries have erected barriers to the free flow of data across borders. Some of these restrictions are intended to stifle dissent and free speech. Some are purely protectionist in nature, or some are for other policy reasons, such as protecting the privacy of a country's citizens.

Today's hearing presents a good opportunity to examine what rules should govern the international flow of data, and what role the United States can play in establishing and enforcing these policies.

When we talk about cross-border data flow, it could be something as simple as someone in a New York office of a multi-national bank and emailing a colleague in the bank's Hong Kong office. It could also be someone sitting in Paris accessing their Facebook account, or logging onto iTunes and downloading movies and songs contained on American servers.

But it also has much more complex applications. Cloud computing allows businesses and consumers to store data and service that could be located anywhere in the world. And some global businesses gather data across their worldwide operations to a centralized location where it can be analyzed to better stream their supply chain or improve service to their customers.

Companies of every shape and size, and across nearly every industry, rely on data that crosses international borders at some point along its journey. That is why it's important that we carefully examine any restrictions that might impede the free flow of data.

Some restrictions, like those that block access to social media or filter out political dissent, are clearly improper, and threaten the human rights of those countries and citizens. America should continue to lead the world in opposing oppressive regimes that stifle the freedom of their people.

Other restrictions, like those requiring a company to process data domestically, or to locate certain infrastructure in-country, are often intended to bolster domestic companies. Many of these restrictions can be removed in the context of trade agreements.

But I have been a persistent critic of some such agreements, in part, because of their devastating impact on American jobs, and we should tread carefully in the digital realm before we make some of the same mistakes we have made with physical goods.

More complicated to address the limitations on data flow, the countries impose to advance other policy goals, like privacy protection. Finding the right balance between protecting the needs of American businesses, respecting the legitimate policies of other Nations, and to ensure that other countries respect ours is not an easy task. That was made clear by the recent decision by the Court of

Justice of the European Union to invalidate the U.S. EU Safe Harbor framework. This important agreement enabled more than 4,000 American businesses to transfer the personal data of EU citizens to the United States if the company certify that they would comply with certain adequacy requirements to protect personal privacy.

The court, however, determined, in part, that because the Safe Harbor scheme only applies to companies and not public authorities, there was not adequate protection for EU citizens from U.S. surveillance activities, and the entire agreement was, therefore, invalidated.

The court also found that EU citizens do not have sufficient remedies under U.S. law if their privacy rights after a transfer are violated.

The gentleman from Wisconsin, Mr. Sensenbrenner, and the distinguished Ranking Member of the full Committee, Mr. Conyers, deserve great credit for working to address the second issue by drafting the Judicial Redress Act, which will provide important privacy protections for EU citizens under U.S. law.

The Judicial Redress Act has already passed the House, and I hope the Senate will take it up shortly. I also appreciate the U.S. Department of Commerce, which is hard at work negotiating a new Safe Harbor Agreement. I hope a new agreement is reached soon, but I also hope that Congress will view this incident as a wake-up call.

The USA Freedom Act took an important step in curtailing surveillance activities, but we should go much further in strengthening our privacy protections. It should not take a European court to prod us into protecting our own citizens.

To ensure that businesses have the flexibility they need, while consumers have the protections they deserve, the United States must work with its partners in the global community to set clear standards governing cross-border data flow. I look forward to discussing what these standards ought to be with our esteemed panel of witnesses today, and I yield back the balance of my time.

Mr. ISSA. The gentleman yields back.

I now recognize the Chairman of the full Committee, Mr. Goodlatte, for his opening statement.

Mr. GOODLATTE. Thank you, Mr. Chairman.

Today's hearing reflects a new twist on the same old song. U.S. companies are at the forefront of the digital economy, and as our companies look to operate globally, they face new and novel non-tariff trade barriers that could make it costly, or near impossible, to operate overseas. As we work to promote digital trade, we must work to make sure that the international playing field is fair. When foreign countries attempt to raise trade barriers ore put in costly regulations as a cost of doing business, we need to call it out for what it is, a barrier to free and fair trade.

We are now in a world where, on one side of the globe, the United States has negotiated the Trans-Pacific Partnership Trade Agreement, with rules promoting cross-border data flows and preventing undue restrictions, such as localization requirements.

And on the other side of the globe, we look at Europe, which has invalidated a 15-year-old Safe Harbor Agreement. This decision translates into uncertainty for thousands of American companies

doing business in Europe, which could have a ripple effect on our economy.

As the United States and Europe continue to negotiate the new Safe Harbor Agreement, we must understand that this is a complex issue for all sides. And we are cautiously optimistic that the Administration and our European allies will be able to come to an agreement that eliminates uncertainty and allows transatlantic commerce to continue.

In the House, we recently passed the Judicial Redress Act. This bipartisan bill, awaiting Senate action, extends certain privacy protections to citizens of European countries, as well as other allied Nations if the Federal Government willfully discloses information in violation of the Privacy Act. Under this bill, citizens of designated countries will be extended the core benefits of the Privacy Act, which already applies to Americans, with regard to information shared with U.S. law enforcement authorities, including the ability to bring a lawsuit for the intentional or willful disclosure of personal information.

This hearing is important because the rules of the road that are considered on digital trade and data flows will either promote or impede the growth of the Internet. A recent BSA report stated that 90 percent of all of the world's data was created in just the last 2 years. While an incredible statistic, it also shows how important data and data flows are to innovation and economic growth.

Localization requirements, such as forcing companies to locate data centers in a particular country, defeat the whole point of cloud computing. New technologies, like The Internet of Things and cloud computing, rely on cross-border data flows. Undue restrictions could prevent companies like Boeing and GE from using IOT sensors in jet engines to send back real-time data to their engineers in the United States.

For global diversified technology and manufacturing companies, they would face the absurd situation of not being able to move their own R&D data from country to country.

Restrictions on data flows fail to recognize the importance of interconnected global supply chains, and the need for the uninterrupted movement of data.

As this Committee continues to study this issue, it is important for us to keep in mind the effects on public policy today and in the future.

I am hopeful that the right policies will help fuel the engine of American innovation, prosperity, and creativity. I think we have a great panel assembled today, and I look forward to hearing from all of our witnesses.

Thank you, Mr. Chairman.

Mr. ISSA. The gentleman yields back. Thank you.

We now will hear from the Ranking Member of the full Committee, the gentleman from Michigan, Mr. Conyers.

Mr. CONYERS. Thank you, Chairman Issa.

I think this is a more important hearing than a lot of people appreciate it. Certainly, that's the case of myself. And to our distinguished list of panelists, we welcome you all, particularly Dr. Atkinson. But I just want to get something out about the digital trade, because the growth of our economy relies on the expansion

of the global digital economy, and efficient cross-border data flow as digital trade becomes a larger portion of the global economy. That's the heart of my introductory comments.

According to the United States International Trade Commission, a digital trade increased U.S. average wages and helped create about 2.4 million full-time positions in 2011, the same year digital trade also increased annual U.S. GDP by 4.8 percent.

As we hear from today's witnesses, which I welcome, I'd like to have considered the following points: To begin with, any discussion on digital trade and unrestricted cross-border data flows requires a serious discussion on surveillance reform. Earlier this year, a coalition of companies, trade associations, civil rights organizations, wrote to the leadership of both parties to outline the economic costs of the significant erosion of global public trust in both the United States Government, and the United States technology sector. Their fears appear to have been prescient.

Last month, citing concerns about insufficient privacy safeguards in the U.S. Court of Justice of the European Union suspended the U.S. EU Safe Harbor framework that allows about 4,400 United States-based companies to move digital information across the Atlantic. The decision is a reminder that we need to have a thorough conversation about surveillance reform. Without one, we cannot fully address eliminating restrictions on cross-border data flow.

A couple of weeks ago, the House took a step toward a fuller discussion by passing H.R. 1428, the Judicial Redress Act, which our colleague, Jim Sensenbrenner, introduced, and I was proud to be a cosponsor of.

The bill extends to the citizens of certain foreign countries, privacy protection, and it will facilitate information-sharing partnerships with law enforcement agencies across the globe. This will save lives.

Although there is far more work to be done, I hope that our allies will take our work on the Judicial Redress Act as a sign of good faith and a first step.

We must continue to work to restore the public trust necessary for the continued success of the United States industry overseas, while protecting individual rights. Digital trade and cross-border data flows are transforming how American consumers and small businesses operate and interact. For example, Ford Motor Company and Boeing, analyze, in real time, digital data from their vehicles and aircrafts. This helps them diagnose problems and quickly find solutions. This saves consumers money and saves lives.

Similarly, small businesses depend on having efficient cross-border data flow in digital trade. For example, digital trade affords them the ability to expand into foreign markets. Consumers rely on online payment processors, like PayPal, to process their payments globally from purchases on online platforms and small businesses.

Finally, the flow of data across international borders presents a unique regulatory setting. Congress, the Administration, foreign governments, and nongovernmental actors, must provide solid consumer protections that safeguard the development of these ever-increasing data flows. The smart and thoughtful discussion I believe we ought have today will be to illuminate barriers to future growth that we need to consider and address. According to studies, restric-

tions like data localization mandates hinder economic development in those companies that erect barriers to digital trade. We should examine how they affect consumers and the United States-based businesses.

Still, some barriers are necessary to protect against the digital trade of illegal goods and services, such as digital piracy and the trafficking of child pornography.

I look forward with interest to having the witnesses at today's hearing, and I thank the Chairman.

Mr. ISSA. Thank you. The gentleman yields back.

Without objection, all——

Mr. CONYERS. Mr. Chairman.

Mr. ISSA. For what purpose does the gentleman seek recognition?

Mr. CONYERS. For the record, I would like to enter into the record an ACLU report concerning the Subcommittee on Courts, Intellectual Property, and the Internet hearing dated November 2, 2015.

Mr. ISSA. Without objection, placed in the record.

Mr. CONYERS. Thank you.

[The information referred to follows:]

WASHINGTON
LEGISLATIVE OFFICE



The Honorable Darrell Issa
Chairman
Subcommittee on Courts, Intellectual Property, and the Internet
Committee on the Judiciary
U.S. House of Representatives
Washington, D.C. 20515

The Honorable Jerrold Nadler
Ranking Member
Subcommittee on Courts, Intellectual Property, and the Internet
Committee on the Judiciary
U.S. House of Representatives
Washington, D.C. 20515

CC: Members of the Judiciary Committee's Subcommittee on Courts, Intellectual Property, and the Internet

RE: House Judiciary Committee's Subcommittee on Courts, Intellectual Property, and the Internet hearing, "International Data Flows: Promoting Digital Trade in the 21st Century."

November 2, 2015

Dear Chairman Issa, Ranking Member Nadler, 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 House Judiciary Committee's Subcommittee on Courts, Intellectual Property, and the Internet hearing, "International Data Flows: Promoting Digital Trade in the 21st Century," to address the E.U.-U.S. Safe Harbor Agreement.

In recent years, the international flow of data has become an essential component of the global economy, facilitating both the growth of U.S. businesses and the free flow of ideas. However, U.S. surveillance practices – which increasingly rely on dragnets that

AMERICAN CIVIL
LIBERTIES UNION
WASHINGTON
LEGISLATIVE OFFICE
915 15th STREET, NW, 6TH FL
WASHINGTON, DC 20005
T/202.544.1681
F/202.546.0738
WWW.ACLU.ORG

FAIZ SHAKIR
DIRECTOR

NATIONAL OFFICE
125 BROAD STREET, 18TH FL.
NEW YORK, NY 10004-2400
T/212.549.2500

OFFICERS AND DIRECTORS
SUSAN N. HERMAN
PRESIDENT

ANTHONY D. ROMERO
EXECUTIVE DIRECTOR

ROBERT REMAR
TREASURER

[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 more than a 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.

collect and review the information of millions of Americans and others around the world – threaten the continued international flow of data.

The impact of U.S. surveillance practices on international data flows was evident in the recent *Schrems* judgment issued by the Grand Chamber of the Court of Justice of the European Union (CJEU)[2]. As part of the decision, the CJEU struck down the legal underpinnings of the E.U.- U.S. Safe Harbor Agreement, which permitted U.S. companies to transfer personal data from the E.U. to the U.S. The judgment was based, in part, on a finding that the legal basis for the arrangement failed to ensure an "adequate level of protection" for E.U. data in the U.S. In its decision, the court referenced the European Commission finding that U.S. authorities were able to access the data of E.U. citizens in the U.S. in a way that was "incompatible...with the purposes for which it was transferred" and "beyond what was strictly necessary and proportionate to the protection of national security."[3]

Currently, U.S. and E.U. policy makers are reportedly negotiating a new Safe Harbor Agreement.[4] However, the *Schrems* judgment makes clear that U.S. surveillance practices must change to enable transatlantic data flow under the auspices of a new Safe Harbor Agreement. Specifically, we believe that before a new Safe Harbor—that can withstand subsequent judicial challenges—can be negotiated, the U.S. must, at a minimum, reform Section 702 of the Foreign Intelligence Surveillance Act (FISA).

Schrems Judgment and Section 702

Since its inception, the ACLU has opposed Section 702 of the Foreign Intelligence Surveillance Act (FISA) – a surveillance law used by the government to search millions of communications of Americans and others around the world. To satisfy the standards set forth in *Schrems*, Congress must reform Section 702 to provide greater protections for data transferred from the E.U. At a minimum, such reforms must include:

- Eliminating Upstream Surveillance:[5]

As the CJEU made clear, surveillance must be necessary and proportionate to a country's national security needs.[6] Upstream surveillance conducted under Section 702 fails this test. Through upstream surveillance, the government taps directly into the Internet backbone inside the United States, which is made up of the cables and switches that carry the communications of hundreds of millions of Americans and others around the world.[7] The National Security Agency (NSA) seizes and copies all of these

[2] Case C-362/14, Schrems v. Data Protection Comm'r, 2000 EUR-Lex 520 (Sept. 23, 2015), available at http://curia.europa.eu/juris/liste.jsf?nd=ALL&language=en&jur=C&parties=Schrems.
[3] *Schrems*, ¶ 90.
[4] Mark Scott, *Data Transfer Pact Between U.S. and Europe is Ruled Invalid*, N.Y. TIMES (Oct. 6, 2015), http://www.nytimes.com/2015/10/07/technology/european-union-us-data-collection.html.
[5] The ACLU is currently engaging in litigation challenging Upstream surveillance as unconstitutional. Wikimedia Found. v. NSA/Central Sec. Serv., 2015 U.S. Dist. LEXIS 144059 (D. Md. Oct. 23, 2015)
[6] While the *Schrems* decision focused on largely on collection under the PRISM program, many of its concerns would similarly apply to the Upstream program. *Schrems*, ¶ 91.
[7] PRIVACY AND CIVIL LIBERTIES OVERSIGHT BOARD, REPORT ON THE SURVEILLANCE PROGRAM OPERATED PURSUANT TO SEC. 702 OF THE FOREIGN INTELLIGENCE SURVEILLANCE ACT (2014) https://www.pclob.gov/library/702-Report.pdf.

communications, searching text-based communications for terms related to its "foreign targets" (as explained further below, these targets may not have any nexus to national security).

It is important to note that, as part of Section 702 surveillance, the Foreign Intelligence Surveillance Court (FISC) does not review whether there is sufficient cause to conduct surveillance on specific targets; nor does it approve the terms that the NSA uses to search text-based communications traversing the Internet. Thus, the NSA is permitted to engage in dragnet surveillance with little judicial oversight. Accordingly, current upstream surveillance fails to satisfy the framework put forward in *Schrems* and will need to be discontinued to permit a valid Safe Harbor Agreement.

- Narrowing the Scope of Section 702 Surveillance

Section 702 permits surveillance for purposes that extend far beyond national security needs or counterterrorism. Under Section 702, the government is not required to certify that surveillance targets are agents of a foreign power, engaged in criminal activity, or even remotely associated with terrorism. Instead, the government is permitted to target any foreigner believed to have "foreign intelligence" information – a term defined broadly to cover a wide array of communications. For example, "foreign intelligence" is defined to include information about foreign affairs, which could include communications between international organizations and government whistleblowers; diplomats; or even journalists and sources. Such surveillance, due to its very purpose, extends beyond what is necessary and proportionate to protect U.S. interests. As a result, Congress must narrow the purpose of Section 702 surveillance, including the definition of "foreign intelligence," to address the concerns highlighted in *Schrems*.

- Providing Effective Redress

The *Schrems* judgment notes that individuals in the E.U. must have access to judicial remedies in cases where they challenge the treatment of their data – something they lack under the current legal framework in the U.S. Recently, the House passed H.R.1428, the "Judicial Redress Act", which sought to extend certain protections in the Privacy Act to citizens of countries designated by the Attorney General. However, the reforms in the Judicial Redress Act, which are exceedingly limited in scope, fail to provide adequate redress to E.U. citizens subject to improper surveillance under Section 702. First, the protections in H.R. 1428 apply only to citizens of countries designated by the Attorney General, and can be revoked at the discretion of the Executive Branch. Second, H.R. 1428 grants only an exceedingly limited set of rights to E.U. citizens under the Privacy Act.[8] Finally, even for citizens of the U.S., the Privacy Act fails to provide an avenue to challenge national security surveillance programs. Thus, to address the concerns in *Schrems*, Congress will need to create a framework for individuals to meaningfully challenge improper surveillance of individual's data stored in the U.S.

- Placing Limits on the Retention and Use of Section 702 Data

The *Schrems* judgment notes that the U.S. lacks rules to limit the interference with the fundamental rights of people in the E.U. whose data is transferred to the U.S. Under Section 702, the government has broad

---

[8] *See*, Letter from Electronic Privacy Information Center (EPIC) to Rep. Bob Goodlatte and Rep. John Conyers on H.R 1428, the Judicial Redress Act of 2015 (Sept. 16, 2015) https://epic.org/foia/umbrellaagreement/EPIC-Statement-to-HJC-on-HR1428.pdf.

authority to retain and use the data of Americans and others around the world. Section 702 permits the retention of any data that constitutes "foreign intelligence," or is encrypted.[9] Even for data that does not fall into either of these categories, the default retention period is five years. In addition, data can be disseminated to other countries, and used for a wide variety of purposes, including criminal prosecution. To address the concerns in *Schrems*, Congress will need to place more stringent restrictions on the access and use of Section 702 data.

Additional Section 702 Reforms

In addition to the reforms noted above, the *Schrems* judgment offers the opportunity for Congress to examine other facets of Section 702 surveillance to address practices that violate the privacy and civil liberties of Americans. Specifically, Congress should, at a minimum, require a warrant before acquiring, accessing, or using Americans' communications; close the "backdoor search loophole" permitting warrantless searching of Section 702 data for information about Americans; ensure standing for litigants to challenge Section 702 surveillance in court; require notice when Section 702 information or evidence derived from it is introduced as evidence in a criminal, civil, or administrative proceeding; provide greater transparency and oversight; and reform the state secrets privilege, which acts as a barrier to judicial review of Section 702.

Addressing these issues is necessary, not only to protect the privacy and civil liberties of Americans and others around the world, but also to permit a new Safe Harbor Agreement that will facilitate transatlantic data flows.

If you have any questions, please feel free to contact Legislative Counsel, Neema Singh Guliani at 202-675-2322 or nguliani@aclu.org.

Sincerely,

Karin Johanson
Director, Washington Legislative Office

Neema Singh Guliani
Legislative Counsel

[9] *See*, Sec. 6 OFFICE OF THE DIR. OF NAT'L INTELLIGENCE, MINIMIZATION PROCEDURES USED BY THE NSA IN CONNECTION WITH ACQUISITIONS OF FOREIGN INTELLIGENCE INFORMATION PURSUANT TO SEC. 702 OF THE FOREIGN INTELLIGENCE SURVEILLANCE ACT OF 1978, AS AMENDED (accessed Nov. 2, 2015) *available at*, http://www.dni.gov/files/documents/ppd-28/2014%20NSA%20702%20Minimization%20Procedures.pdf

Mr. ISSA. You're most welcome.

Without objection, other members' opening statements will be made a part of the record. We now move to our distinguished panel for today.

The witnesses' written statements will be entered into the record in their entirety, and I'd ask you to please summarize, within 5 minutes or less, your opening statement.

To help us stay within the timing, as you may be used to, you will see a red, yellow, and green light in front of you. Please think of them like you do the lights that you never, never run in your daily driving habits.

Before I introduce the witnesses, I would ask that all witnesses please rise to take the oath pursuant to the Committee rules. Raise your right hands.

Do you solemnly swear or affirm that the testimony you're about to give will be the truth, the whole truth, and nothing but the truth?

Please be seated.

Let the record reflect that all witnesses answered in the affirmative.

Our witnesses today include Ambassador Peter Allgeier, president of the Coalition of Service Industries; Dr. Robert Atkinson, president of the Information Technology and Innovation Foundation; Ms. Victoria Espinel, president and CEO of BSA, the Business Software Alliance, or the Software Alliance now as we want to call it; and Mr. Ed Black, president and CEO of the Computer and Communications Industry Association; and certainly never least, Mr. Mark McCarthy, senior vice president of Public Policy for the Software & Information Industry Association.

And with that, we'll go down, starting with the Ambassador. Oh, and before you begin, I would note that we're going to go about 5 or 10 minutes into when the bells ring, and then we'll be gone for roughly half an hour, but we'll try to get through as many witnesses as possible.

Ambassador.

TESTIMONY OF AMBASSADOR PETER ALLGEIER, PRESIDENT, COALITION OF SERVICE INDUSTRIES (CSI)

Mr. ALLGEIER. Thank you very much, Mr. Chairman, Mr. Ranking Member, and Members of the Subcommittee for allowing me to participate in today's hearing.

The global economy today is in the midst of two revolutions that are inextricably linked: The digital revolution and the services revolution. And the United States is in the best position to define the courses of these revolutions, and to benefit from them if we follow appropriate policies, especially in international trade.

Now, the services revolution is evident from the fact that service is, by far, the largest source of jobs, of GDP, and of job growth. And more importantly, they are the enablers of all other sectors of the economy, including manufacturing, agriculture, and energy.

At the center of the service's revolution, however, is the second revolution, the digital revolution. And all services, indeed, all parts of the economy, depend upon digital communication within their own businesses, with their customers, and with their suppliers.

And the Internet, of course, is emblematic of the digital revolution. This revolution has enabled services to be delivered digitally across borders to a degree that was unimaginable two decades ago. But, the international rules and provisions governing trade and services and digital trade have not kept up with these developments. So they urgently need to be updated and brought into line with the realities of a digitally-connected world.

Now, as a number of the members already have said, many countries do not share our entrepreneurial and technological aptitudes and seek to get advantage by imposing legal restrictions on the ability of a firm to manage and move its own data across borders, or they impose requirements to store data on local servers. A common measure by such countries is for the government to require that foreign firms establish facilities for storing and processing their data in the jurisdiction that they are serving.

This tendency is particularly pronounced in regulated sectors such as banking, insurance, and telecommunications.

These localization requirements essentially make cloud computing services impossible. Examples of local data storage and processing requirements abound, just, for example, in Greece, in China, in India, in Russia, in Indonesia, and in Malaysia.

So it is essential that our government oppose attempts, in all sectors, to impose localization requirements on local businesses. The opportunity to do so lies in the various trade negotiations that are occurring now. The Trans-Pacific Partnership, the Transatlantic Trade and Investment Partnership, the Trade in Services Agreement in Geneva, and also work in the World Trade Organization.

These negotiations should set the standards for digital trade by, one, ensuring parties can transfer, access, process and store data across borders; two, prohibiting parties from requiring the establishment or use of local servers; three, ensuring nondiscriminatory treatment of digital products and services from other parties; and four, allowing parties to regulate cross-border data flows for legitimate policy reasons, but only within the accepted standards that are included in the World Trade Organization in the GATS, the General Agreement on Trade in Services.

So how are we doing with respect to using these trade agreements? The TPP has made important progress in advancing the objective of freedom for cross-border data flows and prohibitions on localization requirements. However, it includes one very disturbing exception to the prohibition on localization requirements, and that is that financial services, including banking and insurance, are excluded from the localization prohibition. Every other business has that prohibition in this agreement. But most disturbing is that this exception was at the insistence of the U.S. Government, and this misguided position gives our trading partners the perfect political argument to impose such requirements on our businesses.

What we need to do, in addition to fixing that, is to ensure that we don't repeat that mistake in the negotiations that are taking place elsewhere in the transatlantic negotiations, and in the Trade in Services Agreement.

I'll just make one point about Safe Harbor, because that also is something that is extremely important. Everybody knows that that decision was just handed down by the Court of Justice in Europe.

Our member companies are very eager to work with the Congress and the Administration to find a solution that preserves our companies' ability to move data across the Atlantic, but with appropriate respect for individuals' privacy.

So thank you, Mr. Chairman and members. We very much appreciate the opportunity to be part of this today, and congratulate you on the attention that you are paying to this issue. It's extremely important to the service industry, but also to the economy more broadly. Thank you.

[The prepared statement of Mr. Allgeier follows:]



Testimony of Peter Allgeier
President
Coalition of Services Industries (CSI)

Hearing On
"International Data Flows:
Promoting Digital Trade in the 21st Century"

House Committee on the Judiciary
Subcommittee on Courts, Intellectual Property, and the Internet

November 3, 2015
2141 Rayburn House Office Building
Washington DC

Testimony of Peter Allgeier
President, Coalition of Services Industries (CSI)

Before the House Committee on the Judiciary
Subcommittee on Courts, Intellectual Property and the Internet

Hearing on
"International Data Flows: Promoting Digital Trade in the 21st Century"
November 3, 2015

Good Afternoon, Chairman Issa, Ranking Member Conyers and members of the Subcommittee. My name is Peter Allgeier. I am the President of the Coalition of Services Industries (CSI).

The Coalition of Services Industries (CSI) is the leading industry association devoted exclusively to promoting the international objectives of the U.S. service sector. Our members include the vast array of U.S. companies that provide services domestically and internationally, such as banking, express delivery and logistics, energy, insurance, media and entertainment, retail and wholesale services, technology, telecommunications, and other services sectors. We work globally to obtain solutions to significant international services issues, such as interference in cross-border data flows, unfair competition from state-owned enterprises, domestic content and localization requirements, and lack of transparency and due process in regulatory regimes.

Two Revolutions

The global economy is experiencing two inextricably linked revolutions: the Digital Revolution and the Services Revolution. The United States is in the best position to define the courses of those revolutions and to benefit from them---if we pursue the right policies, especially international trade policies.

The United States is at the forefront of both movements. Our innovations in technology and in business models set the direction and pace of these revolutions. As a result, we are the most competitive supplier of international services in the world. Last year we exported services worth more than $700 billion, resulting in a services surplus of nearly a quarter trillion dollars.

Services Revolution

The Services Revolution is evident from the fact that services by far are the largest source of jobs, output, and job growth. More important is that services are the enablers of all other sectors of the economy, including manufacturing, agriculture and energy. These sectors depend on banking, insurance, computer-related services, logistics, engineering, communications, etc. to achieve their production and income goals. All of these services and other sectors also depend on digital communication within their businesses, with their customers, and with their suppliers. Services and digital communications are critical elements in the operation of global value chains, which are the principal phenomenon in international trade today.

Digital Revolution

At the center of the services revolution is a second revolution: "The Digital Revolution", of which the Internet is emblematic. This has enabled services to be delivered digitally across borders to a degree that was unimaginable twenty years ago. Keep in mind that Amazon.com was only founded in 1994, and Facebook was founded ten years later.

None of this was contemplated twenty years ago when people negotiated the GATS (General Agreement on Trade in Services), the multilateral rules for trade in services that was part of the Uruguay Round in the World Trade Organization. The world has changed radically in the intervening years as a result of technological advances, global data flows, global value chains, innovative business practices, and the widespread use of the Internet by everyone.

The international rules and provisions governing trade in services and digital trade have not kept up with these developments. They urgently need to be updated and brought into line with the realities of today's digitally-connected world.

Internet is the New Great Silk Road

The Internet is the Great Silk Road of the 21st century. Just as the Great Silk Road provided the transmission route for trade among Asia, Europe and North Africa during the 6th thru 14th centuries, the Internet today plays that role for the entire globe.

In this digital age, companies in international markets constantly need to move data digitally across the globe for their own internal operations and in serving their customers.

While this may be obvious in the case of insurance firms processing claims or accounting firms verifying and reviewing audits, it is actually essential for any international business. For example, think of express delivery companies tracking packages across the globe, or an airline company remotely monitoring its engines while the planes are in flight. Retailers have to manage their worldwide procurement and inventory. Health professionals seek second opinions from specialists across the globe.

Many countries that do not share our entrepreneurial and technological aptitudes seek to gain advantage by imposing limits on our businesses' ability to conduct their operations in the most efficient ways possible. Governments increasingly and routinely impose legal restrictions on the ability of a firm to manage and move its own data across borders, or they impose requirements to store data on local servers.

A common reaction by such countries is for the government to require that foreign firms establish facilities for storing and processing their data in the jurisdiction that they are serving. This tendency is particularly pronounced in regulated sectors such as banking, insurance, and telecommunications. Imposing such server localization requirements impede both efficiency and security in handling data. They are the current millennium's version of the Norse King Canute, trying to turn back "the cloud", as he claimed the power to turn back the tide.

Local storage requirements require data which is generated in a country to remain stored on domestic servers. Companies operating in a country with local storage requirements cannot remain competitive in the global market. Local storage requirements increase business costs and induce delays, which make companies' pricing less competitive and more costly for consumers.

Moreover, businesses typically backup data outside the country in which it is collected to ensure that it remains safe and secure in the event of natural disasters, power outages, and other situations that take a data center offline. Preventing data from crossing borders will eliminate the ability to mitigate these risks.

Examples of local data storage and processing requirements abound. For example, Greece, China, India, Russia, Indonesia, and Malaysia all require data generated within the country be stored on servers within the country.

Localization Means No Clouds

Localization requirements essentially make cloud computing services impossible, as it is a portal to outsource both software and hardware in order to increase efficiency, reduce costs, and provide better security of data. In addition, requiring data centers to remain in the country of origin severely limits businesses, both domestic and international, from serving foreign markets.

Digital Trade Must be Central to Negotiations

To be a truly 21st Century trade agreement, negotiations must open borders to digital trade in the same manner in which they open borders to trade in goods and services.

New negotiations should set the standard for digital trade by:

- Ensuring parties can transfer, access, process, and store data across borders;
- Prohibiting parties from requiring the establishment or use of local servers;
- Ensuring non-discriminatory treatment of digital products and services from other parties; and
- Allowing parties to regulate cross-border data flows for legitimate policy reasons only within accepted standards under the GATS Article XIV.

It is essential that our government oppose attempts in all sectors to impose localization requirements on our businesses. The opportunity to do so lies in the various trade negotiations occurring now---the Trans Pacific Partnership agreement (TPP), Transatlantic Trade and Investment Partnership (TTIP), the Trade in Services Agreement (TiSA) and in the World Trade Organization. President Obama has stated clearly that a motivation for the TPP and other negotiations is for the U.S. to exercise the lead in setting the rules for the 21st century. In all of these negotiations, therefore, we should insist on rules that prohibit such localization requirements on any of our businesses.

Assessing Current Trade Agreements and Negotiations

It appears that the TPP negotiations have made important progress in advancing the objective of freedom for cross border data flows and prohibitions on

localization requirements. These provisions are horizontal provisions, so they apply to all economic actors unless one of the parties registers a non-conforming measure (NCM), i.e., a specific legal exception to that obligation. At this point we are not aware of such an NCM.

However, the TPP does include one very disturbing exception to the prohibition of localization requirements. Financial services, which include both banking and insurance, is excluded from the localization prohibition that covers every other business. But most disturbing is that this exception has occurred at the insistence of the United States. This misguided position gives our trading partners the perfect political argument to impose such requirements on our businesses. Yet in the world of cloud computing, the physical location of the data storage and processing makes no difference in the timely access to data by regulators or law enforcement officials. This position is particularly misplaced in that these are among the most highly regulated businesses in our economy, so any delays in providing data to financial regulatory agencies would jeopardize a recalcitrant company's very right to operate.

If we want to maintain our competitiveness and leadership in the midst of the Services and Digital Revolutions, we need to stand firmly against localization requirements in all of our trade relations. The U.S. services industry is eager to work with the Congress and the Administration to ensure that the implementation of TPP and the negotiation of other agreements prevent the various forms of localization requirements.

Beyond the TPP, the U.S. is negotiating the plurilateral Trade in Services Agreement (TiSA) in Geneva and the Transatlantic Trade and Investment Partnership (TTIP) with the European Union. It is essential that we not repeat the mistake in these negotiations that has occurred in the TPP with respect to localization. I hope that this Subcommittee will register its strong opposition to excluding any sector of the economy from the provisions on cross border data flows and the prohibition of localization requirements. The Reports of both the House Ways and Means Committee and the Senate Finance Committee on Trade Promotion Authority state explicitly that financial services should not be excluded from these provisions.

In addition to the challenges of ensuring open digital trade in these trade negotiations, we face a serious threat to trans Atlantic digital and services trade as a result of the recent ruling by the European Court of Justice that the Safe Harbor

Agreement between the U.S. and the European Union is invalid on the grounds of being inconsistent with European data privacy law. The Safe Harbor arrangement is the mechanism that sets the standard under which thousands of firms have been able to transfer data back and forth between Europe and the United States for fifteen years in compliance with European privacy requirements. The European Data Protection Authorities have provided a 90 day moratorium on enforcement of the ruling. It is essential that U.S. and European Commission authorities agree on a legally valid and commercially workable alternative to the existing Safe Harbor. Our member companies are eager to work with the Administration to find a solution that preserves our companies' ability to move data across the Atlantic.

Conclusion:

Our competitiveness and prosperity depend upon embracing the Services and Digital Revolutions in order to create the conditions in which all businesses can benefit from these developments.

CSI and its member companies and their employees congratulate this Subcommittee for its close attention to promoting digital trade and American leadership in its further advancement.

Thank you for the opportunity to appear before the Subcommittee today. I look forward to responding to any questions that Members may have.

Mr. ISSA. Thank you, Ambassador.
Dr. Atkinson.

TESTIMONY OF ROBERT D. ATKINSON, Ph.D., FOUNDER AND PRESIDENT, THE INFORMATION TECHNOLOGY AND INNOVATION FOUNDATION

Mr. ATKINSON. Good afternoon, Chairman Issa, Ranking Member Nadler, Members of the Subcommittee. It's a pleasure to be here today to talk about this critical issue. And in my written testimony, I go into great length and detail on all the economic benefits to both the global and the U.S. economy from cross-border data flows, so I won't go into that too much, but I want to make one point that a couple of others have made, which is, this is not, quote, "just a Silicon Valley thing." Cross-border data flows are critical to a wide variety of industry, mining, agriculture, automobile production, finance, retailers.

So this is really something that's affecting all of our industries, all sizes of companies. And, unfortunately, we don't have the ability to control our own fate here, because a growing number of Nations are engaging in digital protectionism. Some of the policy reasons for them are, perhaps, legitimate in the sense that they have this concern for privacy. In other cases, privacy is a guise for just naked protectionism; they don't want data to flow outside their country in order to benefit their own domestic companies. And in, still, other cases, companies are requiring data to reside in their borders so they can have unfetterred government access to that data without the rule of law.

But whatever the rationale, this data protectionism hurts the U.S. economy. It raises costs for our companies; it makes them have less global market share. That's why in 2013, ITIF estimated that the cost to U.S. technology companies alone from all of the Snowden revelations and the backlash against us and the restrictions that companies—countries were putting in place under the guise of the Snowden revelations, we stood—our technology companies stood to lose anywhere between 21- and $35 billion by next year in revenues, in global revenues. That hurts not just our technology companies, but the U.S. economy and U.S. workers.

So what do we need to do? I think one of the things we cannot do for a lot of, I think, reasons, but one is we cannot simply say that the way to solve this problem is to adopt the most stringent privacy regime in the world. We can't have another region, another country, tell us what our laws and rules should be with regard to privacy. Our view is our privacy rules and policies are actually the reason we lead in the global digital economy, not the other way around. So we cannot have one solution.

The good news is, we don't have to have one solution. The way—we've argued very, very strongly that when a foreign—when a U.S. company operates on foreign soil, they're subject to the laws of that country. They can't just—just by moving data back to the U.S., they can't get out of their legal obligation. They can't then say, well, we're going to use U.S. privacy policies, even though we have a branch in Brussels.

So in a lot of ways, I think this is a lot of much ado about nothing. We can look just, for example, at the Canadian privacy com-

missioner, who has filed a number of successful suits against U.S. companies who have branch plants or facilities in Canada, who have broken, or purportedly, broken Canadian privacy law by moving the data back to the U.S., processing it in a way that was against Canadian rules. The Canadian Government had the ability and the right to bring action against those U.S. companies. They did so, and they prevailed. There's no reason why Europe couldn't do the exact same thing.

So what do we need do? I agree with the Ambassador, we really need to push forward on two steps: The first step being trade agreements. TPP purportedly has—reportedly has strong agreements, protections for digital trade there, TiSA as well. But I think the key challenge there is really making sure that any national security or privacy exceptions are very, very narrow. The risk is that the exceptions won't be narrow, and countries will use this again as a guise to restrict—to restrict data flows.

I also think the U.S. should not be overly defensive, at least on the commercial side of the ledger. We have a right to do what we're doing. Our companies aren't really breaking any laws, by and large. And I think it's time for us to at least put on the table the possibility of a WTO suit against Europe. Europe has, as we all know, cut off our access to data flows to the U.S. because of the Safe Harbor. They have not cut off data flows to Israel; they have not cut off data flows to Argentina, neither—both of those countries still have agreements with Europe, and yet, there is no evidence that the national security protections for government access to that data in Israel or Argentina are any less stringent than ours. If Europe wants to go down this path, they should cut off data flows from every country in the world, not just the United States.

And lastly, we need to—one area we do need to act on is with regard to government access of data. Our companies in America can comply with foreign laws quite well, and when they don't, they can be prosecuted. What they can't comply with is what government does with data. That's why we've proposed that we work with Europe to craft what we call the Geneva convention on the acts on data, where we come up with a set of norms and rules that we would all agree with in terms of government access to data to restore that trust.

Thank you for the opportunity to appear before you today.

[The prepared statement of Mr. Atkinson follows:]

ITIF | INFORMATION TECHNOLOGY & INNOVATION FOUNDATION

Testimony of

Robert D. Atkinson, Ph.D.

Founder and President

The Information Technology and Innovation Foundation

on

"International Data Flows:

Promoting Digital Trade in the 21st Century"

Before the

House Judiciary Committee

Subcommittee on Courts, Intellectual Property, and the Internet

November 3, 2015

INFORMATION TECHNOLOGY AND INNOVATION FOUNDATION | 1101 K STREET NW | SUITE 610 | WASHINGTON, DC 20005
MAIL@ITIF.ORG | (202) 449-1351 | FAX: (202) 638-4922

Good afternoon Chairman Issa, Ranking Member Conyers, and members of the Subcommittee; thank you for inviting me to share the views of the Information Technology and Innovation Foundation (ITIF) on the path to promoting digital trade in the 21st century.

The Information Technology and Innovation Foundation is a non-partisan think tank whose mission is to formulate and promote public policies to advance technological innovation and productivity internationally, in Washington, and in the states. Recognizing the vital role of technology in ensuring prosperity, ITIF focuses on innovation, productivity, and digital economy issues. We have long been involved in the digital trade debate, advocating for policies which support the free flow of data across borders as essential to global trade and commerce and I very much appreciate the opportunity to comment on this issue today.

Since 1944, when the Bretton Woods Conference established the framework for the post-war global economy, there has been a strong, shared consensus that as long as governments do not engage in mercantilist policies, global trade will improve economic welfare. In the manufacturing-based economy of that time, this consensus mainly applied to trade in goods. But as services trade grew, so too did the shared commitment to free trade in services. Now, with the rise of the data economy, it has become clear that free trade in data is just as important to maximizing both U.S. and global welfare as free trade in goods and services, if not more so. The Unired States holds a distinct leadership role in the data economy because it has been a pioneering innovator and early adopter of information technology, so ensuring that there is global free trade in data will be an especially important driver of U.S. economic competitiveness, job creation, wage growth, and consumer benefits.

However, global free trade in data is under serious threat. Many nations, for a variety of motivations—some relared ro privacy and security concerns, many related to naked protectionism—are putting in place policies to balkanize rhe dara economy by limiting cross-border data flows. Even here in the United States, some privacy advocates and opponents of trade are decrying the proposed Trans-Pacific Partnership (TPP) for (rightly) including strong and enforceable provisions against data protectionism.

My testimony will first review why free trade in data is so important to the U.S. economy. I will then document the sizeable and growing threat to free trade in data and explore the different motivations of countries involved. Finally, I will discuss where we stand in terms of progress (e.g., TPP) and setbacks (e.g., the recent decision by the European Court of Justice to reject the longstanding U.S.-EU Safe Harbor Agreement) and propose a number of steps Congress and the administration can take to advance free trade in data.

In short, the task now is for policymakers to continue building on the progress in TPP—next in the context of the Transatlantic Trade and Investment Partnership (T-TIP) and the Trade in Services Agreement (TiSA)—while at the same time alleviating tensions in the law enforcement and national security arena by embracing needed reforms.

Why Data Innovation Is Important

In a growing digital economy, the ability of organizations to collect, analyze, and act on data represents an increasingly important driver of innovation and growth. To start with, the Internet broadly, and data specifically, are key drivers of growth. The McKinsey Global Institute estimates that for 13 of the world's largest economies between 2007 and 2011, the Internet alone accounted for 21 percent of aggregate GDP growth.[1] ITIF has estimated that, all by itself, the commercial activity that is concentrated under the Internet's ".com" top-level domain will contribute $3.8 trillion annually to the global economy by 2020.[2]

Moreover, it is increasingly the case that many of the benefits from information technology come from creating value and insights from data. Virtually every sector of the U.S. economy benefits from the data revolution; the applications for data processing and analytics are so vast that it is difficult to grasp the magnitude of the potential benefits. And this value will only increase as the public and private sectors alike become more data-driven.[3] For example, the McKinsey Global Institute estimates that making open data available for public use, particularly government data, would unlock up to $5 trillion in global economic value annually across just seven sectors, ranging from education to consumer finance.[4] In the United States, the use of big data in health care can save $450 billion per year.[5] Industry forecasters estimate that, by 2025, the Internet of Things will have an economic impact of up to $11.1 trillion per year.[6] And for the global public sector, the Internet of Things is expected to create $4.6 trillion in value by 2022.[7] According to a study by the Lisbon Council and the Progressive Policy Institute, if six of Europe's largest economies (France, Germany, Italy, Spain, Sweden, and the United Kingdom) could raise their "digital density" (the amount of data used per capita) to U.S. levels, those countries could generate an additional €460 billion in economic output per year; a 4 percent increase in their GDP.[8]

Why Free Trade in Data Is Important

A key reality of the global digital economy is that a significant share of data needs to move across borders. It is not unusual, for example, for Internet traffic to go through multiple different intermediaries in multiple nations. To paraphrase cyberspace advocate John Perry Barlow, who once said "information wants to be free," today, "information wants to be global." As the OECD notes in a recent report on the data economy:

> The data ecosystem involves cross-border data flows due to the activities of key global actors and the global distribution of technologies and resources used for value creation. In particular, ICT infrastructures used to perform data analytics, including the data centres and software, will rarely be restricted to a single country, but will be distributed around the globe to take advantage of several factors; these can include local work load, the environment (e.g., temperature and sun light), and skills and labour supply (and costs). Moreover, many data-driven services developed by entrepreneurs "stand on the shoulders of giants" who have made their innovative services (including their data) available via application programming interfaces (APIs), many of which are located in foreign countries.[9]

Indeed, the growing extent and value of cross-border data flows is reflected in the fact that the data-carrying capacity of transatlantic submarine cables rose at an average annual rate of 19 percent between 2008 and 2012.[10]

This is why—absent policy-created "data protectionism"—digital trade and cross-border data flows are expected to grow much faster than the overall rate of global trade. Indeed, Finland's national innovation organization, TEKES, estimates that by 2025, half of all value created in the global economy will be created digitally.[11]

As a result, the ability to move data across borders is a critical component of value creation for organizations in the United States and other countries around the world. As the OECD states, "the free flow of information and data is not only a condition for information and knowledge exchange, but a vital condition for the globally distributed data ecosystem as it enables access to global value chains and markets."[12] Fully half of all global trade in services now depends on access to cross-border data flows.[13] And digitally enabled services have become a key growth engine for the U.S. economy, with exports reaching $356 billion in 2011, up from $282 billion just four years earlier.[14]

This is why the U.S. International Trade Commission (ITC) estimates that digital trade increased annual U.S. GDP by between $517 and $710 billion in 2011 (3.4 to 4.8 percent).[15] The ITC further estimates that digital trade increased average wages and helped create 2.4 million jobs in 2011. U.S. firms in digitally intensive industries sold $935.2 billion in products and services online in 2012, including $222.9 billion in exports. Similarly, based on 2014 estimates, the U.S. International Trade Commission estimated that decreasing barriers to cross-border data flows would increase U.S. GDP by 0.1 to 0.3 percent.[16] And even though the ITC's analysis shows important benefits from digital trade, those benefits are likely understated. This is because the report limited its analysis to "digitally intensive" sectors, which means that its numbers exclude contributions from firms in industries that only use digital trade as a smaller part of their business.

The ITC also found digital trade to be crucial for digitally intensive small and medium-sized enterprises, which sold $227 billion in products and services online in 2012. Indeed, small firms in a wide array of sectors depend on digital trade. For example, in the $120 billion U.S. app industry, small companies and startups account for 82 percent of the top-grossing applications. Consumers throughout the world use these apps and any interruption in cross-border data flows will negatively affect both firms' revenues and customers' experiences.

One reason digital trade is so important to the U.S. economy is that U.S. information technology companies lead the world. As of 2010, U.S. firms held a 26 percent share of the global information technology (IT) industry and were the world's largest producers of IT goods and services.[17] Of the top 20 enterprise cloud computing service providers in the world, 17 are headquartered in the U.S.[18] Of the top 10 Internet firms, seven are U.S.-headquartered.[19]

But as important as free trade in data is to U.S. tech firms, it is even more important to traditional industries, such as automobile manufacturers, mining companies, banks, hospitals, and grocery store chains—all of which depend on the ability to move data across borders or analyze it in real-time as a fundamental enabler of their supply chains, operations, value propositions, and business models. Indeed, among the thousands of U.S. firms that have operated under the U.S.-EU Safe Harbor Agreement, 51 percent do so in order to process data on European employees—for example, transferring the personnel files of overseas workers to the United States for human resource purposes—and most of these firms are in traditional industries.[20] In fact, the McKinsey Global Institute estimates that about 75 percent of the value added by data flows on the Internet accrues to "traditional" industries, especially via increases in global growth.[21]

There are numerous examples of U.S. firms benefiting from cross-border data flows. For example, Ford Motor Company gathers data from over four million cars with in-car sensors and remote applications management software.[22] All data is analyzed in real-time, giving engineers valuable information to identify and solve issues, know how the car responds in different road and weather conditions, and be aware of any other forces affecting the vehicle. This data is returned back to the factory for real-time analysis and then returned to the driver via a mobile app. Like other car companies, Ford believes the data belongs to the owner and they are its "data steward." For internal purposes, performance data is de-identified and analyzed to track potential performance and warranty issues.[23] Ford uses a U.S. cloud service provider to host this data.[24]

Likewise, Caterpillar, a leading manufacturer of machinery and engines used in industries, established its fleet management solution to increase its customers' performance and cut costs. Sensor-enabled machines transmit performance and terrain information to Caterpillar's Data Innovation Lab in Champaign, Illinois where data can be analyzed, enabling Caterpillar and its customers to remotely monitor assets across their fleets in real time. This also enables Caterpillar and its customers to diagnose the cause of performance issues when things go wrong. For example, truck data at one worksite showed Caterpillar that some operators were not using the correct brake procedures on a haul road with a very steep incline. Retraining the operators saved the customer about $12,000 on the project, and company-wide driver incidents decreased by 75 percent. Cross-border data flow restrictions could limit Caterpillar's ability to offer these services in certain markets, such as those that prevent the movement of GPS data across borders.[25]

When nations impose restrictions on data flows, the U.S. economy is harmed in at least two ways. First, requiring localization of data and servers will move activity from the United States to these nations, reducing jobs and investment here and raising costs for U.S. firms. Second, if the restrictions preclude U.S. firms from participating in foreign markets, then U.S. firms will lose global market share to competitors that are based in those protected markets.

Some advocates assert that the U.S. economy can thrive simply by having a healthy small business sector and that policymakers can and should be indifferent to the competitive fate of U.S. multinational corporations. But this is profoundly wrong. Losing global market share because of digital protectionism—regardless of whether it is in information industries or "traditional"

industries—harms not just U.S. multinationals, but also the U.S. economy and U.S. workers. A large body of scholarly literature proves this point. Dartmouth's Matthew J. Slaughter finds that employment and capital investment in U.S. parents and foreign affiliates rise simultaneously.[26] In a study of U.S. manufacturing multinationals, Desai et al., find that a 10 percent greater foreign investment is associated with 2.6 percent greater domestic investment.[27] Another study of U.S. multinational corporation services firms found that affiliate sales abroad increases U.S. employment by promoting intra-firm exports from parent firms to foreign affiliates.[28] In short, when U.S. multinationals are able to expand market share overseas, it creates real economic benefits and jobs here at home. These jobs run the gamut, including sales, marketing, and management—particularly engineering, computer science, and technical jobs. And this matters because, as ITIF has shown, IT workers earned 74 percent more than the average worker in 2011 ($78,584 versus $45,230). In 2011, the IT industry contributed about $650 billion to the U.S. economy, or 4.3 percent of GDP, up from 3.4 percent in the early 1990s.[29]

Finally, digital trade is not just benefiting large companies like Amazon and Ford. Small and medium-sized U.S. enterprises make up one-quarter of digital trade sales and fully one-third of digital trade purchases.[30]

Free trade in data is important not just for businesses and their workers, but for all Americans. Imagine if data had a much harder time crossing borders. Americans traveling overseas would not be able to use their credit cards or cell phones, because both require cross-border data flows. In fact, without cross-border data flows, people would not be able to fly overseas at all, because airlines need to transmit data on passenger manifests and flight operations and governments need to transfer passport data on passengers. People would have a hard time shipping packages overseas. If they get sick while traveling, there would be no way to access their medical records, much less receive remote medical expertise or diagnostic tests, if medical data are not allowed to cross borders. Without data flows, officials can't pre-position travelers' personal information to speed customs and border crossings. And companies would not be able to provide international service or warranty protection over the productive life of a product. For example, it would disrupt the increasingly common practice in which automakers remotely upgrade the software in people's cars.

By contrast, the free flow of data can improve the quality of goods and services, including public goods. For example, cross-border data flows can be an essential component of pandemic disease management and control. The free flow of data is also a key to providing remote diagnostics with medical imaging systems, as there can be personally identifiable information in these systems. Likewise, farmers can remotely receive personalized weather feeds that are based on big data analytics (e.g., a mash up of data on weather forecast and history, soil moisture, soil content, river flows, etc.), but this requires data to be able to flow across national borders.

As a case study, consider how cross-border data flows can impact quality and safety in the airline industry. Aircraft manufacturer Boeing, headquartered in Chicago, relies heavily on data transmitted from planes operating around the world to improve safety and reduce flight delays and cancellations. Boeing has created a system called Airplane Health Management that processes the large amounts of

data that its airplanes generate and transmit in real time while they are in flight.[31] For example, a Boeing 737 engine produces 20 terabytes of data per hour.[32] Commercial airlines that operate Boeing aircraft, such as United Airlines, can monitor this data in real time and proactively dispatch maintenance crews to await an airplane's arrival and quickly address any problems that may have arisen during a flight.[33] Since the very purpose of airplanes is to traverse borders, the success of such a system hinges on Boeing's ability to quickly and easily transmit data from its planes to its airline customers across the globe.[34]

The free flow of data will also enhance overall "data innovation," which will play a key role in improving the lives of Americans. A case in point is medical research. Diseases do not stop at national borders, and the data that are needed to help find cures need to cross borders, too. Powerful data analytics applied to bigger global data sets can help speed the development of cures. (Organizations can "de-identify" data so that they do not release personally identifiable information.) The rarer the disease, the more important it is to collect data on a global basis, since data from individual countries may not create a large enough database to reveal patterns. Unnecessary restrictions on data flows will make it harder for health care providers to save lives.

Finally, it is important to note that support for free trade in data does not have to mean support for the free flow of all data, regardless of its legal status. Just as it is not a violation of free trade principles to block trade in banned products, such as elephant ivory or rhinoceros products, it is also not a violation of free trade principles to oppose digital trade in illegal digital goods, such as child pornography, email spam, Internet malware, and pirated digital content. Numerous countries, including the United Kingdom, Denmark, Greece, Italy, Portugal, and Singapore, have blocked websites that trade in pirated digital content (either using their domain name or network address), thereby preventing that data from flowing into the country.[35] In fact, according to the International Federation of the Phonographic Industry, the global trade association for the music industry, "[Internet service providers] in 19 countries have been ordered to block access to more than 480 copyright infringing websites."[36] This is clearly not digital protectionism. Rather, it is indicative of how the global trading system was intended to work, enabling trade in legal goods, services, and data, and prohibiting trade in illegal goods, services, and data. Moreover, just as taking a stand against trade in products like ivory does not weaken America's intellectual leadership in promoting free trade, taking a stand against trade in illegal digital goods will not weaken our case in promoting free trade in data.

Barriers to Digital Trade

Data will naturally flow across borders when it needs to, unless nations erect digital barriers. Such barriers involve legal requirements on companies to either store and process data locally or to use only local data servers as a condition for providing certain digital services. These non-tariff barriers undermine the benefits of digital trade and make it difficult for U.S. firms to compete with local ones. Troublingly, an increasing number of nations are erecting digital trade barriers.

- In 2014, **Nigeria** put into effect the "Guidelines for Nigerian Content Development in Information and Communications Technology (ICT)."[37] Several of the provisions regard restrictions on cross-border data flows and mandate that all subscriber, government, and consumer data be stored locally.[38]

- **Turkey** passed a law in 2014 mandating that companies process all digital payments inside its borders.

- Two Canadian provinces, **British Columbia** and **Nova Scotia**, have implemented laws mandating that personal data held by public bodies such as schools, hospitals, and public agencies must be stored and accessed only in Canada unless certain conditions are fulfilled.[39]

- **Greece** introduced data localization requirements in February 2011 through a law that states, "Data generated and stored on physical media, which are located within the Greek territory, shall be retained within the Greek territory." The European Commission criticized the law as being inconsistent with the E.U. single market, but it remains in effect.[40]

- **Venezuela** has passed regulations requiring that IT infrastructure for payment processing be located domestically.

- **Malaysia** has passed a local data server requirement, but has not yet implemented it.[41]

- **Australia** requires that local data centers be used as part of e-health record systems.[42] The rationale is to protect Australians' privacy and security. However, as discussed below, mandates on where data is stored do not improve privacy or security. Nevertheless, Australian IT companies have used this fear to promote protectionist policies that spare them from having to compete with U.S. technology companies.

- In 2014, **Indonesia** began considering a "Draft Regulation with Technical Guidelines for Data Centres" that would require Internet-based companies, such as Google and Facebook, to set up local data storage centers.[43] The Technology and Information Ministry is now implementing this regulation under the country's Electronic Information and Transactions (ITE) Law.[44]

- In **Russia**, amendments to the Personal Data Law mandate that data operators that collect personal data about Russian citizens must "record, systematize, accumulate, store, amend, update and retrieve" data using databases physically located in Russia.[45] This personal data may be transferred out, but only after it is first stored in Russia. Even the guidelines for this law, which went into effect in September 2015, acknowledge that there are significant ramifications for foreign companies due to this law.

- Many are also concerned that **Europe** will introduce data protectionist policies as part of its Digital Single Market, General Data Protection Regulation, and European Cloud initiatives.[46]

- In **Vietnam**, a Decree on Information Technology Services requires digital service providers or websites to locate at least one server within Vietnam. Vietnam had also put forth a draft IT Services Decree that would include additional data localization requirements as well as restrictions on cross-border data flows.

- **India** has considered a measure that would require companies to locate part of their ICT infrastructure within the country to provide investigative agencies with ready access to encrypted data on their servers.[47] In February 2014 the Indian National Security Council proposed a policy that would institute data localization by requiring all email providers to setup local servers for their India operations and mandating that all data related to communication between two users in India should remain within the country.[48]

- In **South Korea**, the Personal Information Protection Act requires companies to obtain consent from "data subjects" (i.e., the individuals associated with particular datasets) prior to exporting that data.[49] The act also requires "data subjects" to be informed who receives their data, the recipient's purpose for having that information, the period that information will be retained, and the specific personal information to be provided. This is clearly a substantial burden on companies trying to send their data across borders.

- Not surprisingly, given its history of rampant "innovation mercantilism," **China** is putting in place a wide array of protectionist measures on data. To start with, it has long limited data "imports." For example, the Ministry of Public Security runs the Golden Shield program (commonly referred to as the "Great Firewall of China"), which restricts access to certain websites and services, particularly ones that are critical of the Chinese Communist Party. But more importantly from a trade perspective, China has made a number of moves in the wake of the Snowden revelations to restrict the cross-border transfer of data.[50] For example, Chinese law prohibits institutions from analyzing, processing, or storing off-shore personal financial, credit, or health information of Chinese citizens. A recent set of draft administrative regulations for the insurance industry included localization requirements, both for data centers and cross-border data flows. Furthermore, China's Counter-Terrorism Law requires Internet and telecommunication companies and other providers of "critical information infrastructure" to store data on Chinese servers and to provide encryption keys to government authorities.[51] Any movement of data offshore must undergo a "security assessment." And China's draft cybersecurity law would require IT hardware to be located in China. China's policy framework to develop a domestic cloud computing capability also refers to the importance of regulating cross-border data flows.

Countries' Motivations for Limiting Free Trade in Data

Despite the vast benefits to companies, workers, consumers, and economies that arise from the ability to easily share data across borders, dozens of countries—in every stage of development—have erected barriers to digital free trade.[52] There are three main motivations for this: privacy and security concerns, national security and law enforcement concerns, and aspirations for economic growth. In almost all cases, though, more than one motivation plays a role.

For example, Europe's concerns about data trade stem in large part from its desire to protect citizens' privacy (although as noted below there are some in Europe who want to use these concerns as a justification for data protectionism in an effort to grow Europe's IT sector). As discussed below, effectively addressing privacy concerns should be the easiest of the three motivations to address. First, as ITIF has shown, requiring data not to leave a nation does little to increase privacy.[53] As long as the company involved has legal nexus in a European nation, it is subject to EU laws and regulations; moving data outside the EU does not give the company a free pass to ignore EU law. Moreover, the EU and the United States have long had a workable Safe Harbor agreement to address precisely these kinds of privacy concerns. And the European Court of Justice overturned the Safe Harbor not because of privacy concerns, but because of concerns about governmental access.

If privacy were the only motivation for Europe to restrict transatlantic data flows, then there should be no reason why Europe and America cannot work out a mutually agreeable solution. To be sure, compared to the United States, Europe has different laws and values with regard to privacy. But there are misconceptions about this on both sides of the Atlantic. Too many Americans believe EU privacy rules exclude even the most basic uses of data for commercial purposes and innovation, and too many Europeans believe that the United States is a "wild west" of data privacy. In fact, both sides share similar values with regard to privacy, the rule of law, and government access to data, and both benefit enormously from globalization and data innovation.

A second motivation for governments to require data to stay in country concerns the ability of governments to get access to data. This appears to be a motivation for many non-democratic governments, such as Russia and China, requiring that data be stored inside their borders. There is no question that localization policies such as these give government security services easier access to data. However, those nations do not need to mandate localization for their governments to legal access to data. They are still able to compel companies doing business in their markets to turn over data even if it is stored outside their nation. In truth, even this is not enough for some governments; they want the power to collect data without the knowledge of the company involved, and that is easier if the data are stored locally. For democratic nations that abide by the rule of law, there is no need for mandating data be stored domestically as long as there is a well-functioning and robust system of mutual legal assistance treaties (MLATs) in place as described below.

Finally, a number of countries see "data mercantilism" as a path to economic growth, because they believe (incorrectly) that if they restrict data flows they will gain a net economic advantage from data-related jobs.[54] And all too often they are spurred on by domestic IT companies seeking an unfair leg up over foreign competitors. For example, Australian businesses have used privacy and

security fears to promote protectionist policies that spare them from having to compete with U.S. tech companies. When Rackspace, a Texas-based cloud computing firm, built its first data center in Australia, MacTel—a domestic competitor—tried to stoke fears of U.S. surveillance efforts under the Patriot Act to push Rackspace out of the market.[55] In fact, this same Australian company funded a report calling on Australian policymakers to impose additional regulations designed to put foreign cloud computing competitors at a disadvantage.[56]

Similarly, some calls in Europe for data localization requirements aud procurement prefereuces for European providers, and even for a so-called "Schengen area for data"—a system that would keep as much data in Europe as possible—appear to be motivated by digital protectionism.[57] For example, Germany has started to create a dedicated national network, called "Schlandnet."[58] And Deutsche Telecom is pushing the European Commission to adopt rules making it harder for U.S. cloud providers to operate in Europe in order for them to gain market share. Similarly, the French government has gone so far as to put €150 million into two start-ups, Numergy and Cloudwatt, to build domestic cloud infrastructure that is independent of U.S. tech companies.[59] French Digital Economy Minister Fleur Pellerin explains that France's goal is to locate data servers and centers in French national territory and to "build a France of digital sovereignty."[60]

But any economic benefits for countries from digital protectionism are far outweighed by the costs. Such requirements raise ICT costs not only by forcing companies to locate servers in locations that may not be the most cost-effecrive; they also force companies to operate ar sub-optimal economies of scale. Barriers to cross-border data transfer for cloud computing add significant costs for local companies. Studies show that local companies would need to pay 30 percent to 60 percent more for their computing needs.[61] Businesses that move their cloud computing outside the European Union could save more than 36 percent because they could use global best in class providers.[62]

These increased costs are eventually passed along to dara users, including businesses. As ITIF has shown, elasticity is quite high with information and communications technologies—ranging from 1 to 3—meaning that for every 1 percent increase in ICT costs, there is a 1 percent to 3 percent reducrion in ICT consumprion.[63]

Barriers ro cross-border data flows can also stop research and development between a company and a foreign partner as they are not able to share all the data relevant to developing new services or processes.[64] For example, companies may not be able to use cloud computing to connect different research and development unirs. These barriers may force multinational companies to use second-best research partners. All of these factors hinder innovation.

This is why a 2013 report by the European Center for International Political Economy (ECIPE) estimated that if cross-border data flows were seriously disrupted, the negative impact on EU GDP would be between 0.8 percent and 1.3 percent.[65] This study also showed that the negative economic impact of recently proposed or enacted cross-border data flow restrictions would be substantial in a number of other nations, including Brazil, China, India, Indonesia, South Korea, and Vietnam. Likewise, a study into the impact of Russia's data localization laws shows an estimated economic loss

of 0.27 percent of GDP, equivalent to $5.7 billion, and a 1.4 percent decrease in investment.[66] But despite these costs, many nations persist in data protectionism.

Costs to the U.S. Economy of Foreign Digital Protectionism

As described above, the U.S. economy and U.S. workers benefit from cross-border data flows, in part because the United States is the global leader in the data economy. Foreign restrictions will impose costs on U.S. companies in a wide variety of industries. But particularly damaging are the costs to U.S. IT companies. One reason is that a number of nations have used the Snowden revelations as an excuse to impose protectionist data policies that will disproportionally hurt U.S. tech firms. In 2014, one survey of businesses in the United Kingdom and Canada found that 25 percent of respondents planned to pull company data out of the United States as a result of the National Security Agency (NSA) revelations.[67] As a result, U.S. tech firms have seen losses across the world. For example, the U.S. cloud company Salesforce faced major short-term sales losses and suffered a $124 million deficit following the initial NSA revelations.[68] Cisco also saw its sales interrupted in Brazil, China, and Russia because of reports that the NSA had secretly inserted backdoor surveillance tools into its routers, servers, and networking equipment.[69] These reports damaged the company's international reputation and prompted it to take extra precautions to thwart surreptitious actions by the NSA.[70] IBM, Microsoft, and Hewlett-Packard also have reported diminished sales in China as a result of the NSA revelations.[71]

In 2013, ITIF estimated that if concerns about U.S. surveillance practices caused even a modest drop in the expected foreign market share for cloud computing services, it could cost U.S. technology companies between $21.5 billion and $35 billion by 2016.[72] It has since become clear that not just the cloud computing sector but the entire U.S. tech industry has underperformed as a result of the Snowden revelations. Therefore, the economic impact of from the Snowden revelations will likely far exceed ITIF's initial $35 billion estimate.[73] Indeed, other estimates have put the figure somewhere around $47 billion.[74] As noted above, these costs are borne by U.S. workers and the U.S. economy overall, not just by tech company shareholders.

Where Are We Now?

The last few months have seen mixed progress on establishing movement toward free trade in data. On the one hand, the proposed TransPacific Partnership significantly advances the cause. But on the other, the European Coutt of Justice's invalidation of the U.S.-EU Safe Harbor agreement is a significant setback.

The digital trade provision in the Trade Promotion Authority Bill rightly puts the issue of cross-border data flows at the top of U.S. trade negotiators' agenda.[75] Reflected in the U.S. Trade Representative's top priorities for digital trade, which it refers to as the "Digital Dozen," these disciplines are necessary elements for trade agreements to promote an open Internet and an Internet-enabled economy.[76]

The TPP's e-commerce chapter is reported to contain rules explicitly prohibiting restrictions on cross-border data flows and data localization requirements. Ideally, the TPP should expand and strengthen the trade rules achieved under the e-commerce chapter of the Korea-United States FTA (KORUS), which included an agreement that both countries "shall endeavor to refrain from imposing or maintaining unnecessary barriers to electronic information flows across borders."[77] There has also been progress through the Asia Pacific Economic Community (APEC) process. In November 2011, APEC Leaders issued a directive to implement the APEC Cross Border Privacy Rules System (CBPR). The CBPR system balances the flow of information and data across borders while at the same time providing effective protection for personal information. The system is one by which the privacy policies and practices of companies operating in the APEC region are assessed and certified by a third-party verifier (known as an "Accountability Agent") and follows a set of commonly agreed upon rules, based on the APEC Privacy Framework. The Privacy Recognition for Processors (PRP) was recently endorsed by APEC in January 2015 and will be operationalized in the coming months. The PRP is designed to help personal information processors assist controllers in complying with relevant privacy obligations, and helps controllers identify qualified and accountable processors.

At the same time, when the European Court of Justice decided in early October 2015 to allow the High Court of Ireland to invalidate the U.S.-EU Safe Harbor agreement, it signaled that the Snowden revelations had called into question the mutual understanding that both parties share the basic goal of protecting their citizens' privacy in a digital world, even though they go about it differently—the EU, by adhering to comprehensive legislation, and the United States by taking a sector-by-sector approach that relies on a mix of legislation, regulation, and self-policing. Europeans have become wary because their laws provide a fundamental right to privacy, and they now believe that they are not getting an equivalent level of protection from the United States government. There is now a real risk of contagion as other nations look at the EU decision and decide – for privacy or protectionist motivations – to restrict data flows between the U.S. and their nation. Indeed, reportedly, Israel has also ruled that it would now not recognize that data transferred from Israel to the United States was covered under the EU-US Safe Harbor, as it previously had.[78]

But while European citizens and policymakers are understandably concerned about government access to their citizens' data, abruptly revoking the Safe Harbor agreement was the wrong way to address those concerns. It is disrupting not just to the thousands of U.S. and European companies that currently depend on the Safe Harbor to do business across the Atlantic, but also to the broader digital economy. Policymakers in the United States and EU should instead work together to swiftly implement an interim agreement so the court's ruling does not continue to adversely affect transatlantic digital commerce. At stake is the future viability of the world's most important economic relationship: If it is to continue flourishing in the age of digital commerce, then both sides must make accommodations.

Policy Steps to Enable Digital Free Trade

In many nations, trade negotiators are working to build an international consensus and enforceable regime for the free flow of data across borders. However, at the same time, law enforcement and intelligence communities are seeking to preserve or extend their access to data. These two goals are in fundamental tension and unless nations can put in place a reasonable and consistent framework to govern lawful government access to data, nations will be more likely to restrict cross-border data flows and trade, commerce, law enforcement, and intelligence gathering will all suffer. Indeed, the turbulence in the system now underscores the urgency of addressing these issues, both in terms of advancing new trade regimes to establish enforceable rules for free trade in data and in crafting international standards for government access to data.

The first step in shaping this new system will be to ensure that the U.S. government works to embed strong cross-border data flow protections in new trade agreements. The Obama administration has worked to enshrine strong and enforceable cross-border digital trade provisions in the TPP. But that agreement only applies to 12 nations. So the United States now needs to champion a Trade in Services Agreement (TiSA) that builds upon this language and to persuade as many nations as possible to sign on. TiSA currently covers 23 countries that represent 75 percent of the world's $44 trillion services market.

As the United States moves forward with Europe to negotiate the Transatlantic Trade and Investment Partnership, it will be important for U.S. trade negotiators to insist that strong cross-border provisions be included. Indeed, if the T-TIP is truly going to be a "21st century trade agreement," it must give data flows the same level of consideration it would have given manufacturing in a 20th century agreement.

But because data is so critical to the modern global economy, the United States and European Union should push further to protect the free and unfettered movement of data across the globe—for example by championing a "Data Services Agreement" at the World Trade Organization, which would commit participating countries to protect cross-border data flows and prevent signatory countries from creating barriers to them. It would be akin to the Information Technology Agreement (ITA)—which 54 countries commendably agreed to expand with 201 new product lines earlier this year—for cross-border data flows.

A key challenge to achieving a strong outcome in negotiations on upcoming trade agreements will be ensuring that privacy and national security exemptions are specific and narrow enough to ensure that members are not able to use these as an excuse for digital protectionism. These exemptions under existing international agreements, such as the General Agreement on the Trade in Services (GATS), are so vaguely defined and poorly enforced as to provide a huge loophole for data protectionism. Both issues are obviously legitimate public policy objectives for members and are common exemptions in trade agreements, but the challenge for negotiators is to ensure that the various parts of an agreement (such as on protecting personal information) are strong enough as to allow a stronger regime on cross-border data flows and localizatiou.

In addition, those who argue that free trade provisions for data abrogate national privacy rules, and therefore should not be included in trade agreements, overlook the reality that data does not need to be stored locally to be secure or to maintain privacy protections, as ITIF has shown in a detailed report, *The False Promise of Data Nationalism*.[79]

With regard to privacy, it is important to understand that entities with legal nexus in another nation must adhere to the privacy laws that nation imposes when they leverage consumers' data in the course of their business activities; thus, where that data is stored is immaterial. It is either in compliance with the privacy laws and regulations of that nation, or it is not. For example, foreign companies operating in America must comply with the privacy provisions of the Health Insurance Portability and Accountability Act (HIPAA), which regulates U.S. citizens' privacy rights for health data, or the Gramm-Leach-Bliley rules regulating the privacy of financial data, whether they store a customer's data on their own server in the United States or on a third-party cloud server in another nation.[80] Likewise, there is no benefit to data security by mandating local data storage. Just as with privacy, companies cannot avoid a nation's data security requirements by simply storing data in another nation.

At the same time the United States pushes for stronger, broader, and more enforceable trade regimes on cross-border data protection, it must also lead on reform of government access to data. Otherwise, many nations will likely use the concern of government "snooping" as an excuse to restrict cross-border data flows, even if they have signed a trade agreement covering the issue.

In the pre-Internet era, with Westphalian borders, it was much easier to define a U.S. person versus a non-U.S. person. But when data can be generated, stored, and accessed from anywhere in the world, this old territory-based system is in need of significant modernization. If, for example, the U.S. government asserts that it has authority to compel U.S. technology companies to turn over data on a non-U.S. person that is stored overseas, then the end result will either be that countries will prohibit data from being stored with U.S. technology companies, or that market forces will lead in this direction, as domestic IT companies will market themselves as "NSA-proof." In either case, the U.S. intelligence community will have less access and U.S. technology companies will lose global market share, costing jobs here at home.[81]

To start with and to address European concerns about privacy protections for their citizens' data, the U.S. Senate should follow the House of Representatives' lead and pass the Judicial Redress Act, which would allow non-U.S. citizens in select nations to bring civil actions against the U.S. government if it violates the Privacy Act. Congress also should reform the Foreign Intelligence Surveillance Act to improve oversight, transparency, and accountability whenever the government gets a warrant to collect private data for national security purposes.

The United States should also take the lead in strengthening the Mutual Legal Assistance Treaty (MLAT) process so that, where appropriate, law enforcement can gain access to data overseas.

MLATs are agreements designed for law enforcement agencies to receive and provide assistance to their counterparts in other countries. The United States has MLATs with 64 nations.[82] Despite these arrangements, U.S. law enforcement agencies have complained that MLATs involve a "slow and cumbersome" process.[83] The best option for addressing these challenges is to strengthen the MLAT process so that it is not, as the government argues, too slow, and so that companies cannot take actions to make it difficult for government investigators to gain lawful access to data. The U.S. government should take the lead in creating a timely and efficient international framework for allowing governments to request access to data stored abroad. This framework would help meet the needs of law enforcement agencies operating in a digital world and keep the U.S. tech sector competitive globally by making border distinctions inconsequential for legitimate law enforcement requests. In addition, one immediate step in this direction is to bring the MLAT process into the digital age by creating a streamlined, online docketing system for all MLAT requests.[84]

To build on that, the United States and European Union should also lead in creating a "Geneva Convention on the Status of Data," as ITIF writes in *The False Promise of Data Nationalism.* The purpose of such a convention would be to resolve international questions of jurisdiction and transparency regarding the exchange of information. This would allow for the development of global rules on data sharing and ensure that legitimate concerns regarding privacy and cybersecurity are taken into account as cross-border data flows increase.

This multilateral agreement would establish specific rules for government transparency, create better cooperation for legitimate government data requests, and limit unnecessary access to data on foreign citizens. It would also settle questions of jurisdiction when companies encounter conflicting rules, assist nations in reassuring individuals at home and abroad that the era of mass electronic surveillance unencumbered by effective judicial oversight is at an end, and better hold nations accountable for respecting basic civil liberties. And just as the principles of the Geneva Convention are taught to soldiers in basic training, the principles of a Geneva Convention for Data should be taught to network administrators and IT professionals worldwide, thereby ensuring that the ethics of the agreement are embedded at all levels of industry and government.

Also, it is important for government to not oppose strong encryption to ensure consumers have access to secure technologies without government backdoors. FBI director James Comey reignited a long-running controversy recently when he argued that the encryption U.S. technology companies such as Apple and Google use on their devices could impede law enforcement's ability "to prosecute crime and prevent terrorism."[85] Comey wants U.S. tech companies to design a way for law enforcement officials to access the data stored on those devices. In addition to raising the obvious privacy and government overreach issues, this proposal would also weaken the security and global competitiveness of U.S. tech products.

It is understandable that law enforcement agencies, accustomed to a world where they can open mail and monitor phone calls easily, are nervous about unbreakable encryption. However, these agencies must accept the premise that some communication networks, especially those used by the most elite

criminals and terrorists, will inevitability "go dark."[86] If the U.S. government insists on backdoors in domestic products, those criminals and terrorists intent on avoiding surveillance will simply use devices made in countries that allow less vulnerable encryption. Rather than fight the tide of progress, law enforcement officials should work to find viable alternatives, such as analysis of other data sources and metadata, to solve and prevent crimes.

Europe has reforms to make, too, including fully embracing its planned digital single market. Individual members of the EU should not be able to set their own privacy rules or other digital policies, nor should they be able to overrule laws and regulations established at the European level, because that would fragment the digital marketplace and raise costs for consumers and businesses, as is happening now with the rejection of the safe harbor. More broadly, the purpose of establishing a digital single market cannot be to create a "fortress Europe" where European technology companies have an unfair leg up on foreign competitors. It should instead be the first step toward a more seamlessly integrated transatlantic market.

If the United States and Europe do not come together to resolve their differences on these data privacy and security issues, then both sides will suffer. U.S. companies need to be able to store and process European data in the United States, and vice versa, or it will harm all sorts of technology users, including small businesses and consumers. The berter alternative is to build a durable privacy framework that provides the necessary safeguards and instills the requisite trust and confidence to drive long-term growth on both sides of the transatlantic digital economy.

Most urgently, now that the United States and Europe have settled the Umbrella Agreement for exchanging data related to criminal activities, policymakers should also finish the process of creating a Safe Harbor 2.0 with terms that give comfort to all parties. In particular, the updated agreement should reflect the EU request that a national security exception is used only to the extent that it is strictly necessary and proportionate for a given incident.

At the same time U.S. policy makers should insist that other nations not use variations in privacy laws as a justification for limiting free trade in data, whether policy makers in these nations are doing so out of a sincere concern for privacy or whether they are using privacy as a guise for data protectionism. If the EU precedent stands only one of two outcomes are possible. The first is that all nations will have to put in place domestic privacy rules as strict as Europe's, or in fact, as strict the nation with the strictest rules in the world. Otherwise, the nation with the strictest rules will simply say that data cannot leave its nation. To be sure, this is an outcome that most U.S. privacy advocates relish, for they have long advocated that the United States adopt EU-style privacy laws, ignoring the real economic and inuovation costs that would come from doing so. Aud now they are using this breakdown to push their innovation-restricting policy agenda. But as noted above, it is a "red herring" to assert that the only way to protect commercial privacy and security of a nation's citizens' data is to restrict the export of that data. Moreover, the United States should not allow other nations to dictate U.S. laws and regulations about the Internet—doing so sets a dangerous precedent for other policy issues such as freedom of expression. The second possible outcome is that nations will

effectively levy a privacy tariff" on all companies in nations that do not adopt their rules, as they will have to use more complex and costly arrangements to transfer data across borders. Neither solution is acceptable in a global economy.

As such, if European policy makers are not willing to expeditiously come to a new agreement that allows data to flow relatively easily across the Atlantic, the United States Trade Representative should consider filing a WTO case against Europe. Striking down the Safe Harbor agreement protection was not only arbitrary and capricious but wrong. Europe has invalidated the Safe Harbor agreement with the United States on the grounds that EU citizen data is not safe from government access, but it still maintains that other nations with similar laws and practices provide adequate protection. Moreover, if anything, EU citizen data is safer from government access in the United States than it is in nations like Argentina and Israel, yet European privacy authorities and courts have not revoked data sharing agreements with either of those nations.

In conclusion, we need to protect the ability of individuals and companies to engage in data-driven commerce without geographic restrictions. Companies are using data in creative and wondrous ways to create new value for the global economy. Policymakers must be equally visionary in shaping rules that protect citizens' rights to privacy, without unduly encumbering data's catalytic economic growrh and innovation potential. America's ability to grow its economy and jobs will depend on it.

Thank you again for this opportunity to appear before you today.

Endnotes

1. Stephen Ezell, "Digital Trade Act of 2013 Instrumental to Protecting and Empowering the Global Digital Economy," *Innovation Files*, December 12, 2013, http://www.innovationfiles.org/digital-trade-act-of-2013-instrumental-to-protecting-and-empowering-the-global-digital-economy/.
2. Robert D. Atkinson, Stephen Ezell, Scott Andes, and Daniel Castro, "The Internet Economy 25 Years After .com," (Information Technology and Innovation Foundation [ITIF]), March 5, 2010), https://itif.org/publications/2010/03/15/internet-economy-25-years-after-com.
3. Daniel Castro and Travis Korte, "Data Innovation 101: An Introduction to the Technologies and Policies Supporting Data-Driven Innovation" (Center for Data Innovation, November 4, 2013), http://www2.datainnovation.org/2013-data-innovation-101.pdf.
4. James Manyika et al., "Open data: Unlocking innovation and performance with liquid information" (McKinsey Global Institute, October 2013), http://www.mckinsey.com/insights/business_technology/open_data_unlocking_innovation_and_performance_with_liquid_information.
5. Peter Groves et al., "The big-data revolution in US health care: Accelerating value and innovation" (McKinsey & Company, April 2013), http://www.mckinsey.com/insights/health_systems_and_services/the_big-data_revolution_in_us_health_care.
6. James Manyika et al., "Unlocking the potential of the Internet of Things" (McKinsey Global Institute, June 2015), http://www.mckinsey.com/insights/business_technology/the_internet_of_things_the_value_of_digitizing_the_physical_world.
7. Joseph Bradley et al., "Internet of Everything: A $4.6 Trillion Public-Sector Opportunity" (Cisco, 2013), http://internetofeverything.cisco.com/sites/default/files/docs/en/ioe_public_sector_vas_white%20paper_121913final.pdf.
8. Paul Hofheinz and Michael Mandel, "Uncovering the Hidden Value of Digital Trade" (The Lisbon Council/Progressive Policy Institute, 2015), http://www.lisboncouncil.net/publication/publication/127-uncovering-the-hidden-value-of-digital-trade-towards-a-21st-century-agenda-of-transatlantic-prosperity.html.
9. Organization for Economic Cooperation and Development (OECD), "Data-driven Innovation, Big Data for Growth and Well—being," (OECD, October 2014), 73, http://www.oecd.org/sti/inno/data-driven-innovation-interim-synthesis.pdf.
10. Michael Mandel, "Data, Trade, and Growth" (Progressive Policy Institute, April 2014), http://www.progressivepolicy.org/wp-content/uploads/2014/04/2014.04-Mandel_Data-Trade-and-Growth.pdf.
11. Ministry of Employment and the Economy, Industrial Competitiveness Approach (Helsinki: Ministry of Employment and the Economy, March 2013), 28.
12. OECD, "Data-driven Innovation, Big Data for Growth and Well—being," 109.
13. Stephen Ezell, "Data a Key Driver of Transatlantic Economic Growth," *Innovation Files*, July 23, 2015, http://www.innovationfiles.org/data-a-key-driver-of-transatlantic-economic-growth./.
14. Stephen Ezell, "Digital Trade Act of 2013 Instrumental to Protecting and Empowering the Global Digital Economy," *Innovation Files*, December 12, 2013, http://www.innovationfiles.org/digital-trade-act-of-2013-instrumental-to-protecting-and-empowering-the-global-digital-economy/.
15. *Digital Trade in the U.S. and Global Economies, Part 2*, United States International Trade Commission, August 2014, http://www.usitc.gov/publications/332/pub4485.pdf.
16. Ibid.
17. National Science Board (NSB), *Science and Engineering Indicators 2012*, (NSB, 2012), appendix table 6-13, Value added of ICT industries, by region/country/economy: 1990–2010.
18. International Trade Administration (ITA), *2015 Top Market Report Cloud Computing* (ITA, July 2015), http://trade.gov/topmarkets/pdf/Cloud_Computing_Top_Markets_Report.pdf.
19. Shobhit Seth, "World's Top 10 Internet Companies," *Investopedia*, March 4, 2015, http://www.investopedia.com/articles/personal-finance/030415/worlds-top-10-internet-companies.asp.
20. European Commission, "Communications from the Commission to the European Parliament and the Council on the Functioning of the Safe Harbor From the Perspective of EU Citizens and Companies Established in the EU," (European Commission, November 27, 2013), http://ec.europa.eu/justice/data-protection/files/com_2013_847_en.pdf.
21. Matthieu Pélissié du Rausas et al., "Internet matters: The Net's sweeping impact on growth, jobs, and prosperity," (McKinsey Global Institute, May 2011), http://www.mckinsey.com/insights/high_tech_telecoms_internet/internet_matters.
22. Mark van Rijmenam, "Ford Drives In The Right Direction With Big Data," *Datafloq*, July 5, 2015, https://datafloq.com/read/ford-drives-direction-big-data/434.
23. Doug Henschen, "Microsoft Azure Drives Ford Hybrid-Cloud Plan," InformationWeek, March 18, 2015, http://www.informationweek.com/strategic-cio/digital-business/microsoft-azure-drives-ford-hybrid-cloud-plan/d/d-id/1319533.
24. Jason Hiner, "How Ford reimagined IT from the inside-out to power its turnaround," *TechRepublic*, July 9, 2012, http://www.techrepublic.com/blog/tech-sanity-check/how-ford-reimagined-it-from-the-inside-out-to-power-its-turnaround/.

25. Business Roundtable, "Putting Data to Work" (Business Roundtable, 2015), http://businessroundtable.org/sites/default/files/reports/BRT%20PuttingDataToWork.pdf.
26. Matthew J. Slaughter, "How U.S. Multinational Companies Strengthen the U.S. Economy" (The United States Council Foundation, Spring 2009), http://www.uscib.org/docs/foundation_multinationals.pdf.
27. Mihir A. Desai, C. Fritz Foley, and James R. Hines Jr., "Domestic Effects of the Foreign Activities on U.S. Multinationals" *National Bureau of Economic Research* (May 2008), http://www.people.hbs.edu/ffoley/fdidomestic.pdf.
28. Jitao Tang and Rosanne Altshuler, "The spillover effects of outward foreign direct investment on home countries: evidence from the United States" (Oxford University Centre for Business Taxation, January 2015), http://www.sbs.ox.ac.uk/sites/default/files/Business_Taxation/Docs/Publications/Working_Papers/Series_15/WP1503.pdf.
29. U.S. Bureau of Economic Analysis, GDP-by-Industry Accounts (value added by industry, accessed December 12, 2012), http://www.bea.gov/iTable/index_industry.cfm; Robert J. Shapiro and Aparna Mathur, "The Contributions of Information and Communication Technologies To American Growth, Productivity, Jobs and Prosperity," (Sonecon, September 2011), http://www.sonecon.com/docs/studies/Report_on_ICT_and_Innovation-Shapiro-Mathur-September8-2011-1.pdf.
30. U.S. International Trade Commission, *Digital Trade in the U.S. and Global Economies, Part 2*.
31. John Maggiore, "Remote Management of Real-Time Airplane Data" (Boeing, 2007), http://www.boeing.com/commercial/aeromagazine/articles/qtr_3_07/AERO_Q307_article4.pdf.
32. Maggiore, "Remote Management of Real-Time Airplane Data"; Paul Mathai, "Big Data: Catalyzing Performance in Manufacturing" (Wipro, 2011), http://www.wipro.com/documents/Big%20Data.pdf.
33. Maggiore, "Remote Management of Real-Time Airplane Data."
34. Daniel Castro and Alan McQuinn, "Cross-Border Data Flows Enable Growth in All Industries" (ITIF, February 2015), http://www2.itif.org/2015-cross-border-data-flows.pdf?_ga=1.174884642.1240521073.1404749065.
35. The International Federation of the Phonographic Industry (IFPI), *Digital Music Report 2015, Charting the Path to Sustainable Growth* (IFPI, April 27, 2015), http://www.ifpi.org/downloads/Digital-Music-Report-2015.pdf.
36. Ibid.
37. Nigeria Federal Ministry of Communication Technology, *Guidelines for Nigerian Content Development in Information and Communications Technology (ICT)*, (Nigeria Federal Ministry of Communication Technology, 2013), http://www.nitda.gov.ng/documents/Guidelines%20on%20Nigerian%20Content%20Developmenet%20in%20ICT%20updated%20on%2012062014.pdf.
38. Ibid.
39. "No Transfer, No Trade" (Kommerskollegium (Swedish National Board of Trade, January 2014), 35, http://www.kommers.se/Documents/dokumentarkiv/publikationer/2014/No_Transfer_No_Trade_webb.pdf.
40. Business Roundtable, "Promoting Economic Growth through Smart Global Information Technology Policy: The Growing Threat of Local Data Server Requirements" (Business Roundtable, June 2012), 5, http://businessroundtable.org/uploads/studies-reports/downloads/Global_IT_Policy_Paper_final.pdf .
41. Ibid.
42. James Stamps and Martha Lawless, *Digital Trade in the U.S. and Global Economies, Part 1* (U.S. International Trade Commission, July, 2013), http://www.usitc.gov/publications/332/pub4415.pdf.
43. Matthias Bauer, Hosuk Lee-Makiyama, Erik can der Marel, and Bert Verschelde, "The Costs of Data Localization: Friendly Fire on Economic Recovery" (European Centre for International Political Economy, March 2014), http://www.ecipe.org/media/publication_pdfs/OCC32014__1.pdf.
44. Eli Sugarman, "How Emerging Markets' Internet Policies Are Undermining Their Economic Recovery," *Forbes*, February 12, 2014, http://www.forbes.com/sites/elisugarman/2014/02/12/how-emerging-markets-internet-policies-are-undermining-their-economic-recovery/.
45. "Russia's Personal Data Localization Law Goes Into Effect" (Duane Morris, October 16, 2015), http://www.duanemorris.com/alerts/russia_personal_data_localization_law_goes_into_effect_1015.html?utm_source=Mondaq&utm_medium=syndication&utm_campaign=View-Original.
46. Nigel Cory, "The Architect of Europe's Digital Single Market Leaves Important Questions Unanswered on U.S. Visit," *Innovation Files*, October 2, 2015, http://www.innovationfiles.org/the-architect-of-europes-digital-single-market-leaves-important-questions-unanswered-on-u-s-visit/.
47. Business Roundtable, "Promoting Economic Growth through Smart Global Information Technology Policy."
48. Thomas K. Thomas, "National Security Council proposes 3-pronged plan to protect Internet users," *The Hindu Business Line*, February 13, 2014, http://www.thehindubusinessline.com/info-tech/national-securitycouncil-proposes-3pronged-plan-to-protect-internet-users/article5685794.ece.

49. Nnupam Chandler and Uyen Le, "Breaking the Web: Data Localization vs. the Global Internet" *Emory Law Journal* (April 2014), 40, http://papers.ssrn.com/sol3/papers.cfm.
50. Robert Atkinson, Stephen Ezell, and Michelle Wein, "Localization Barriers to Trade: Threat to the Global Economy" (ITIF, September, 2013), http://www2.itif.org/2013-localization-barriers-to-trade.pdf.
51. AmCham China, "Protecting Data Flows in the US-China Bilateral Investment Treaty" (AmCham China 2015 Policy Spotlight Series, April, 2015), http://www.amchamchina.org/policy-advocacy/policy-spotlight/data-localization.
52. Ezell, Atkinson, and Wein, "Localization Barriers to Trade: Threat to the Global Innovation Economy."
53. Daniel Castro, "The False Promise of Data Nationalism" (ITIF, December 2013), http://www2.itif.org/2013-false-promise-data-nationalism.pdf.
54. For more information on mercantilism, see Michelle Wein, Stephen Ezell, and Robert Atkinson, "The Global Mercantilist Index: A New Approach to Ranking Nations' Trade Policies" (ITIF, October 2014), http://www2.itif.org/2014-general-mercantilist-index.pdf.
55. Adam Bender, "Patriot Act could apply to Rackspace data in Australia: Privacy advocates," *Computerworld*, August 27, 2012, http://www.computerworld.com.au/article/434683/patriot_act_could_apply_rackspace_data_australia_privacy_advocates/.
56. The report notes: "The United States Patriot Act brazenly declares the US Government's right to access anything it wants from any cloud infrastructure over which it can claim jurisdiction. That creates a demand for cloud computing services that are not subject to such capricious hazards…the Australian government should regulate the cloud so that we're a preferred provider for firms, governments and other users offshore." See: Lateral Economics, "The potential for cloud computing services in Australia" (Lateral Economics, October 2011), http://www.lateraleconomics.com.au/outputs/The%20potential%20for%20cloud%20computing%20services%20in%20Australia.pdf
57. Jeanette Seiffert, "Weighing a Schengen zone for Europe's Internet data," *Deutsche Welle*, February 2, 2014, http://www.dw.de/weighing-a-schengen-zone-for-europes-internet-data/a-17443482.
58. Ibid.
59. Leila Abboud and Paul Sandle, "Analysis: European cloud computing firms see silver lining in PRISM scandal," *Reuters*, June 17, 2013, http://www.reuters.com/article/2013/06/17/us-cloud-europe-spying-analysis-idUSBRE95G0FK20130617.
60. Chandler and Le, "Breaking the Web: Data Localization vs. the Global Internet."
61. Leviathan Security Group, "Quantifying the Cost of Forced Localization" (Leviathan Security Group, 2015), https://static1.squarespace.com/static/556340ece4b0869396f21099/t/559dad76e4b0899d97726a8b/1436396918881/Quantifying+the+Cost+of+Forced+Localization.pdf.
62. Ibid., 10.
63. Robert D. Atkinson and Ben Miller, "Digital Drag: Ranking 125 Nations by Taxes and Tariffs on ICT Goods and Services," (ITIF, October 2014), http://www2.itif.org/2014-ict-taxes-tariffs.pdf?_ga=1.3078388.571485694.1368547120.
64. Kommerskollegium, "No Transfer, No Trade."
65. Bauer et al., "The Costs of Data Localization: Friendly Fire on Economic Recovery."
66. Matthias Bauer, Hosuk Lee-Makiyama, Erik can der Marel, and Bert Verschelde, "Data Localisation in Russia: A Self-imposed Sanction" (European Centre for International Political Economy, June 2015), (http://www.ecipe.org/app/uploads/2015/06/Policy-Brief-062015_Fixed.pdf.
67. "NSA Scandal: UK and Canadian Businesses Wary of Storing Data in the U.S." *PEER 1 Hosting*, January 8, 2014, http://www.peer1.com/news-update/nsa-scandal-uk-and-canadian-businesses-wary-storing-data-in-us.
68. Andrew Mouton, "Salesforce loses money, but masters art of distraction," *USA Today*, December 2, 2013, http://www.usatoday.com/story/tech/2013/12/02/salesforce-earnings/3803095/.
69. Aarti Shahani, "A Year After Snowden, U.S. Tech Losing Trust Overseas," *National Public Radio*, June 5, 2014, http://www.npr.org/sections/alltechconsidered/2014/06/05/318770896/a-year-after-snowden-u-stech-losing-trust-overseas.
70. Jeremy Kirk, "To avoid NSA, Cisco delivers gear to strange addresses," *Computerworld*, March 19, 2015, http://www.computerworld.com/article/2899341/to-avoid-nsa-cisco-delivers-gear-to-strangeaddresses.html.
71. Danielle Kehl et al., "Surveillance Costs: The NSA's Impact on the Economy, Internet Freedom & Cybersecurity," (New America Foundation, July 2014), https://www.newamerica.org/downloads/Surveilance_Costs_Final.pdf.
72. Daniel Castro, "How Much Will PRISM Cost the U.S. Cloud Computing Industry," (ITIF, August 2013), http://www2.itif.org/2013-cloud-computingcosts.pdf.
73. Daniel Castro and Alan McQuinn, "Beyond the USA Freedom Act: How U.S. Surveillance Still Subverts U.S. Competitiveness," (ITIF, June 2015), http://www2.itif.org/2015-beyond-usa-freedom-act.pdf?_ga=1.110906501.1240521073.1404749065.
74. Ed Ferrara and James Staten with Andrew Bartels, Glenn O'Donnell, and Josh Blackborow, "Government Spying Will Cost US Vendors Fewer Billions Than Initial Estimates," *Forrester*, April 1, 2015, https://www.forrester.com/Government+Spying+Will+Cost+US+Vendors+Fewer+Billions+Than+Initial+Estimates/fulltext/-/E-res122149.

75. Ian Fergusson, *Trade Promotion Authority (TPA) and the Role of Congress in Trade Policy* (U.S. Congressional Research Service, June 15, 2015), https://fas.org/sgp/crs/misc/RL33743.pdf.
76. United States Trade Representative's Office (USTR), "The Digital Dozen"(USTR, May 1, 2015), https://ustr.gov/sites/default/files/USTR-The_Digital_Dozen.pdf.
77. United States Trade Representative's Office, "United States – South Korea Free Trade Agreement – Chapter Fifteen – Electronic Commerce" (USTR), accessed October 29, 2015, https://ustr.gov/sites/default/files/uploads/agreements/fta/korus/asset_upload_file816_12714.pdf.
78. Francoise Gilbert, "Israel Revokes Acceptance of Safe Harbor," http://www.francoisegilbert.com/2015/10/israel-revokes-is-acceptance-of-safe-harbor/.
79. Emma Woollacott, "Leaked TISA Documents Reveal Privacy Threat," *Forbes*, June 4, 2015, http://www.forbes.com/sites/emmawoollacott/2015/06/04/leaked-tisa-documents-reveal-privacy-threat: Castro, "The False Promise of Data Nationalism."
80. Stephen Ezell, "Why Privacy Alarmists Are Wrong About Data Rules in Big Trade Deals," *Christian Science Monitor*, July 15, 2015, http://www.csmonitor.com/World/Passcode/Passcode-Voices/2015/0715/Opinion-Why-privacy-alarmists-are-wrong-about-data-rules-in-big-trade-deals.
81. Daniel Castro, "Cross-Border Digital Searches: An Innovation-Friendly Approach," *InformationWeek*, September 5, 2014, http://www.informationweek.com/strategic-cio/digital-business/cross-border-digital-searches-an-innovation-friendly-approach/a/d-id/1306989.
82. U.S. Department of State, *2015 International Narcotics Control Strategy Report, Bureau of International Narcotics Control Strategy Report* (U.S. Department of State, 2015), http://www.state.gov/j/inl/rls/nrcrpt/2015/vol2/239045.htm.
83. Preet Bharara and Lorin Reisner, "Government's Memorandum of Law in Opposition to Microsoft's Motion," *Washington Post*, April 20, 2014, accessed October 30, 2015, http://www.washingtonpost.com/r/2010-2019/WashingtonPost/2014/06/10/National-Security/Graphics/Government%27s Memorandum of Law in Opposition to Motion to Vacate (doc 97....pdf.
84. This is a key provision in the Law Enforcement Access to Data Stored Abroad Act (LEADS Act) currently before Congress.
85. David Sanger and Matt Apuzzo, "James Comey, F.B.I. Director, Hints at Action as Cellphone Data Is Locked," *New York Times*, October 16, 2014, http://www.nytimes.com/2014/10/17/us/politics/fbi-director-in-policy-speech-calls- dark-devices-hindrance-to-crime-solving.html?_r=0; Craig Timberg, "Newest Androids will join IPhones in offering default encryption, blocking police," *Washington Post*, September 18, 2014, https://www.washingtonpost.com/news/the-switch/wp/2014/09/18/newest-androids-will-join-iphones-in-offering-default-encryption-blocking-police/.
86. Valerie Caproni, "Statement Before the House Judiciary Committee, Subcommittee on Crime, Terrorism, and Homeland Security," (Federal Bureau of Investigations, February 17, 2011), http://www.fbi.gov/news/testimony/going-dark-lawful-electronic-surveillance-in-the-face-of-new-technologies.

Mr. ISSA. And thank you.

Ms. Espinel. Sorry. Ms. Espinel. I do that. I apologize. Thanks. Victoria.

TESTIMONY OF VICTORIA ESPINEL, PRESIDENT AND CEO, BSA | THE SOFTWARE ALLIANCE

Ms. ESPINEL. Thank you, Mr. Chairman, Ranking Member, and Members of the Subcommittee.

Mr. ISSA. Try—Victoria, pull it a little closer to see if that works.

Ms. ESPINEL. Maybe mine is off. Can I borrow yours? Thank you.

Mr. ISSA. These are very effective.

Ms. ESPINEL. Thank you. My name is Victoria Espinel, and thank you for the opportunity to testify today on behalf of BSA | The Software Alliance. Promoting international trade by eliminating barriers for cross-border data flows is a top priority for us and for our members. And today's hearing presents a tremendous opportunity to explore three areas: First, the growing importance of data and digital trade; second, forward-looking efforts to expand such trades through agreements like the Trans-Pacific Partnership, and troubling recent developments in Europe and other markets that could derail these potential opportunities.

International trade is critical to our members, and as is the case for many other sectors, international trade for our members increasingly involves data services and digital, rather than physical transactions. The economic implications of the software-enabled data revolution are enormous. Economists predict that making better use of data could lead to a data dividend of $1.6 trillion in the next 4 years. And that efficiency gains alone could add almost $15 trillion to the global GDP by 2030. That's an amount that's equal to the current economy of the United States.

But beyond the economic implications, data is central to the lives of billions of people around the world. Farmers use data to reduce pesticides in water use while increasing yields; families are cutting down on their commute times; cities are redesigning transportation routes that save time and reduce pollution; doctors are using data to save the lives of premature babies and do research on Alzheimer's; people around the world are using data to improve their lives.

Because the actual processing and analysis of data often takes place in various locations that are miles, or even continents apart, it is critically important to be able to move data freely across national borders. And as excited as BSA members are about the potential for software and data-driven innovation to spur growth, we are deeply concerned about steps that several U.S. trading partners have considered, or taken to erect barriers to digital trade and cross-border data flows, including Brazil, Nigeria, China, Russia, and many others.

These barriers take many forms. Sometimes they expressly require the data stay in country, or they impose unreasonable conditions in order to send it abroad, and other cases, they require the use of domestic data centers or other equipment.

In light of the troubling growth and barriers to data flows, BSA members welcome the recently concluded TPP. We understand, based on briefings and discussions with U.S. and TPP partners,

that the agreement include several commitments that are vital to digital trade.

First, robust commitments on cross-border data flows, including explicit prohibitions on data and server localization mandates; second, a prohibition against imposing custom duties on digital products; and third, prohibitions against requiring companies to disclose software service code as a condition of competing in the market.

This is the first time that strong enforceable rules on data have been included in the FTA agreement, and it is a historic opportunity. We look toward to studying carefully the final text, and to working with the Administration and Members of Congress as the agreement moves forward.

While we are pleased by the important rules that the TPP will provide with many of our transpacific trading partners, we are concerned about potential new obstacles that have recently arisen with our biggest transatlantic trading partner, the European Union.

As the Subcommittee is aware, the European Court of Justice recently handed down a decision that invalidates the Safe Harbor, a mechanism that nearly 5,000 U.S. companies of all sizes have relied on for more than a decade, to facilitate digital commerce with customers, suppliers, and partners in Europe. The invalidation of Safe Harbor has broad ramifications with transatlantic trade, not only for software, but for many other sectors of the economy as well.

The current situation has led to uncertainty for Europeans and American individuals and the businesses that serve their needs and the millions of customers that are served by them. We encourage Congress and the U.S. Government to respond with urgency and focus. And we thank each and every member of this Committee for their vote or Judicial Redress Act, and we hope that the Senate follows your lead.

Our members work hard to build privacy and security into their products and services, and are committed to protecting the data in their care, regardless of where that data originates. We are ready to work with Congress and the U.S. Government and with the EU and its member states, to ensure that data continues to move across our borders for the benefit of both Americans and Europeans.

Thank you, again, for providing this opportunity to share our views on these important matters, and I look forward to your questions.

[The prepared statement of Ms. Espinel follows:]



Hearing on

**"International Data Flows:
Promoting Digital Trade in the 21st Century"**

**House Committee on the Judiciary
Subcommittee on Courts, Intellectual Property, and the Internet**

**November 3, 2015, at 1:00 p.m.
2141 Rayburn House Office Building
Washington, DC**

**Testimony of Victoria Espinel
President and CEO
BSA | The Software Alliance**

Testimony of Victoria Espinel
President and CEO, BSA | The Software Alliance
Hearing on "International Data Flows: Promoting Digital Trade in the 21st Century"
November 3, 2015
Washington, DC

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

BSA is the leading advocate for the global software industry in the United States and around the world.[1] Promoting international trade by eliminating barriers to cross-border data flows is a top priority for BSA and its members. I commend this Subcommittee for holding a hearing on this important topic, and I welcome this opportunity to testify on BSA's behalf.

I. **Digital Trade and Data**

For several BSA members, half or more of their revenues today come from overseas—a figure that will almost certainly grow as more developing markets move up the economic ladder. Removing barriers to trade is therefore essential to BSA members' long-term success. As in many other sectors, international trade for our members increasingly involves data services and digital rather than physical transactions. Data services, including, storage, processing, analytics are the fastest growing elements of digital trade. And even how software is used and delivered is changing rapidly. Whereas BSA members once delivered their software to consumers on CD-ROMs or pre-installed on PCs, today software is more often downloaded online or provided remotely, such as through cloud computing services.

The transformation to data services and digital delivery model provides tremendous benefits to users. Data services and software delivered online tends to be extremely flexible, highly scalable, and allows customers to access massive computing power quickly and at a small fraction of what they would pay to store and process the data or run the software themselves. It also gives even small firms the ability to reach a global customer base and engage in cutting-edge innovation. As a result, we—and the billions of customers across the world who rely on our software to run their businesses—increasingly depend on digital trade in order to compete and succeed.

In fact, these software and data services already have become central to the lives of millions of people around the world. Farmers are reducing use of pesticides and water, while improving yields by five or 10 bushels an acre. Families are cutting down their drive times, and cities are designing transportation routes that save time and reduce emissions. Doctors are using data analysis to speed up diagnoses for their patients and make treatments more accurate. People rely on these services to improve their lives.

These myriad transformations also make the ability to move data freely from one place to another of critical importance. That's because most software applications that people use today—whether mobile apps, online productivity tools, or enterprise cloud computing services—involve the user creating or receiving data on his or her device, but the actual processing and analysis of that data occurring elsewhere—somewhere that may be miles or even continents away. This can only happen, however, if data can move freely from one location to another.

[1] BSA's members include Adobe, Altium, ANSYS, Apple, Autodesk, Bentley Systems, CA Technologies, CNC/Mastercam, DataStax, Dell, IBM, Intuit, Microsoft, Minitab, Oracle, salesforce.com, Siemens PLM Software, Symantec, Tekla, The MathWorks and Trend Micro. *See* www.bsa.org.

Likewise, as BSA explains in a recent paper,[2] as the cost of data collection and storage have plunged and innovations in data analytics software have accelerated—innovations that BSA members are actively driving—people and organizations across the economy are finding powerful new ways to use data to produce valuable insights that save time, money and even lives. This too requires data to move freely—whether across town or across the globe.

Indeed, when one looks at the sheer quantity of data that is produced, transferred, and processed today, the numbers are staggering. Already an estimated 2.5 quintillion bytes of data are generated every day.[3] That's enough in a year to fill a stack of DVDs that would stretch from Earth to the moon and back.[4] In fact, more than 90 percent of all the data in the world has been generated in just the last two years.[5] We also are now doubling the rate at which data is produced every two years.[6] By 2019, global IP traffic is projected to exceed 2.0 zettabytes per year—that's over two *trillion* gigabytes of data.[7]

Of course, all this data has little value if it doesn't lead to new knowledge. But by combining human ingenuity with innovative software, people increasingly are able to use these massive volumes of data to find new insights and discover new trends and relationships.

The implications of this software and data revolution are enormous. Economists predict that making better use of data could lead to a "data dividend" of $1.6 trillion in the next four years, and that data-enabled efficiency gains could add almost $15 trillion to global GDP by 2030.[8] As noted in a recent report by the McKinsey Global Institute, "[t]he ability to monitor and manage objects in the physical world electronically makes it possible to bring data-driven decision making to new realms of human activity—to optimize the performance of systems and processes, save time for people and businesses, and improve quality of life."[9]

In addition to driving economic growth and improving the quality of life, these developments will also create jobs. Already, 61 percent of senior executives in the United States say that data analytics is important to their companies' plans to hire more employees.[10] And for every data-related IT job created, another three jobs are estimated to be created for people outside of IT—creating millions more jobs throughout the economy.[11]

II. Barriers to Digital Trade

As excited as BSA members are about the potential for software and data-driven innovations to spur growth, we are deeply concerned about steps several U.S. trading partners have taken to erect barriers to digital trade and cross-border data flows. In countries from Australia, Brazil, Nigeria, and China to Russia, Switzerland, and Vietnam—along with many others—we are seeing a growing trend by governments to impose requirements that make it difficult or impossible to transfer data outside the country.

---

[2] *See* BSA, *What's the Big Deal With Data?* (Oct. 2015), at http://data.bsa.org/wp-content/uploads/2015/10/bsadatastudy_en.pdf.
[3] *Id.* at 7.
[4] *Id.* at 8.
[5] *Id.* at 6.
[6] *Id.*
[7] Cisco, *Cisco Visual Networking Index: Forecast and Methodology, 2014-2019 White Paper* (May 2015), at http://www.cisco.com/c/en/us/solutions/collateral/service-provider/ip-ngn-ip-next-generation-network/white_paper_c11-481360.html.
[8] *See* BSA, *supra* n. 2, at 14.
[9] McKinsey Global Institute, *The Internet of Things: Mapping the Value Beyond the Hype* 1 (June 2015), at http://www.mckinsey.com/insights/business_technology/the_internet_of_things_the_value_of_digitizing_the_physical_world.
[10] BSA, *supra* n. 2, at 14.
[11] *Id.* at 14.

These data market access barriers requirements take many forms. Sometimes they expressly require data to stay in-country or impose unreasonable conditions in order to send it abroad; in other cases, they require the use of domestic datacenters or other equipment. Sometimes they are justified as necessary to spur the local economy, or protect privacy, or to obtain jurisdiction over these services. But too often, there is also an element of protectionism, as the means chosen by these governments tend to be significantly more trade-restrictive than necessary to achieve any legitimate public policy goal.

Given our nation's competitive advantage in data services and software, there is no doubt that these data localization measures hurt U.S. businesses and workers. By prohibiting U.S. companies from transferring the data they collect in one country to a datacenter in another, or combining that data with other data, these measures undermine the enormous efficiencies of scale that online software and data analytics make possible. They also make it more difficult for U.S. companies to offer services that necessarily involve cross-border transfers of data. And because the analysis of large datasets often reveals insights that smaller datasets do not, these measures undermine data innovation and the many economic and social benefits that can flow from such innovation.

As harmful as data localization measures are for U.S. companies and workers, they are equally if not more harmful to the economies of the governments that impose them. By depriving local companies of unfettered access to the tremendous innovations that U.S. companies have to offer, and limiting these companies' ability to engage in data-driven innovation, these governments risk isolating their own businesses, consumers, and economies from the full benefits of the global economy.

III. Recent Developments: TPP and the EU-U.S. Safe Harbor

A. Trans-Pacific Partnership Agreement

In light of the troubling growth in data localization measures and other barriers to digital trade, BSA members welcome the recently concluded Trans-Pacific Partnership Agreement (TPP). Although we have not yet seen the final text, we understand that the Agreement includes several commitments that are vital to digital trade:

- Cross-border data flows. First, we understand the text includes robust commitments on cross-border data flows, including explicit prohibitions on data- and server-localization mandates. We also understand that these commitments are subject to narrow exceptions, so that measures impeding cross-border data flows can be justified only if required to achieve a legitimate public policy objective. These commitments would mark a significant milestone in international law and set a new global standard for promoting trade in digital and data-driven products and services.

- No digital customs duties or discrimination. We also understand that the final text prohibits TPP countries from imposing customs duties on digital products, and from imposing measures that discriminate against digital products as compared to physical products. Given the strength of the United States' digital economy and the competitive advantage we enjoy in many sectors that rely on digital commerce and data flows, this prohibition will be of tremendous benefit to U.S. companies, workers, and consumers.

- No forced source code disclosure. We understand that the final TPP text also prohibits TPP countries from requiring companies to disclose software source code as a condition of competing in the market. For many companies today—not just those in the software sector—the innovations they offer to customers and through which they gain a competitive edge are embodied in software. Protecting these innovations against misappropriation through forced source code disclosure will help ensure that U.S. companies can compete fairly and on a level playing field across all TPP markets.

- Promoting a free and open Internet. Finally, we understand that the final text enshrines the United States' strong commitment to a free and open Internet by affirming the principle that consumers should be able to access online content and applications of their choice for legitimate commercial purposes. Given the Internet's growing importance to economic growth across all sectors of the economy, preserving the free and open Internet is vital to both our values as a nation and to our economic future.

  In an innovation-driven economy such as ours, these protections are vital. We look forward to studying carefully the final text of the Agreement once it is released, and to working with Members of Congress and the Administration as the Agreement moves forward.

B. EU-U.S. Safe Harbor

While we are pleased by the important protections that the TPP will provide with regard to trade with many of our trans-Pacific trading partners, we are concerned by potential new barriers that recently have arisen with our biggest trans-Atlantic trading partner, the European Union.

As this Subcommittee is aware, the EU's Court of Justice recently handed down a decision that invalidates the EU-U.S. Safe Harbor, a mechanism that thousands of U.S. companies have relied on for more than a decade to facilitate digital commerce with customers, suppliers, and partners in Europe. Under longstanding EU law, personal information—which includes a wide range of data—generally can be moved to third countries only if the data is subject to "adequate" protections in those countries, and the EU does not consider the U.S. to be "adequate." The U.S.-EU Safe Harbor Framework, which was adopted in 2000, was designed to allow companies to self-certify that they would provide these "adequate" protections to EU-originating data stored in the United States.

In striking down the Safe Harbor, the Court of Justice focused on issues around national security and law enforcement access to data. Troubled by the Snowden leaks, the Court concluded that countries that permit "indiscriminate surveillance and interception" and "mass and undifferentiated accessing" of personal data could not be deemed "adequate" under EU law.

The invalidation of the Safe Harbor has broad ramifications for trans-Atlantic trade, not only for the technology sector, but for many other sectors of our economy as well. For 15 years, thousands of American and European companies relied on the Safe Harbor mechanism to do business with each other and to set up operations and serve customers in each market. This included companies from a wide range of industries, among them pharmaceutical, aviation, retail, consumer goods, automotive and even agri-business firms. These companies utilized the Safe Harbor to serve European customers and do business with European partners, as well as to make use of our world-class datacenter capabilities and innovative data analytics services. Many routine commercial dealings between the U.S. and European companies have now been disrupted, and customers in Europe are asking hard questions about their ongoing ability to do business with the United States.

Significantly, the European Court's judgment relates only to the Safe Harbor. There are a number of other mechanisms available under EU law that enable the lawful transfer of data from Europe to the United States that our companies are relying on today. Worryingly, however, the long-term stability of these alternative mechanisms is unclear. European data protection authorities have indicated that they are scrutinizing these mechanisms for compliance with EU law following the Court's judgment. German data protection authorities recently announced that they will no longer authorize certain transfers to the United States that they were previously willing to authorize. Countries outside the EU are watching closely; Swiss authorities, for example, have now said that the U.S.-Swiss Safe Harbor, which mirrors the U.S.-EU Safe Harbor, no longer constitutes a sufficient legal basis for data transfers under Swiss law.

The current situation has led to uncertainty for European and American businesses. If the United States and European Union do not act quickly to address this uncertainty, the impact on trans-Atlantic trade could be significant. One study predicts that if data flows from Europe were brought to a near-halt, imports of services into the European Union from the United States could decrease by between 16.6 and 24 percent.12

We encourage Congress, and the U.S. Government broadly, to respond with urgency and focus. European data protection authorities are reviewing the overall framework for EU-U.S. data transfers now and will issue their findings shortly; they have announced a grace period on enforcement until January 31, 2016. Many companies today are working hard to put in place alternatives to transfer data lawfully without certainty that these alternatives will not later be challenged.

U.S. policymakers need to engage immediately with their European counterparts to restore trust and efficiency to trans-Atlantic data flows. Specifically, we need three things: rapid consensus on a new agreement to replace the Safe Harbor, ideally delivered within 90 days; sufficient time to come into compliance with new rules; and a framework in which the European Union and United States can develop and agree a sustainable, long-term solution that reflects and advances the interests of all stakeholders. This will require active engagement, trans-Atlantic dialogue, creative thinking, and a willingness on both sides to listen and meaningfully respond to each other's concerns.

BSA's members are totally committed to protecting data in their care, regardless of where that data originates, and to providing solutions that give individuals robust control over their information. Our members work hard to build privacy and security into their products and services from day one. We are ready to work with Congress and the U.S. Government, and with the governments of Europe, to ensure that data continues to flow across our borders to the benefit of both Americans and Europeans.

* * * * *

Thank you again Chairman Issa, Ranking Member Nadler, and members of the Subcommittee for providing this opportunity to share BSA's views on this important matter. I look forward to answering any questions you might have.

[12] ECIPE, "The Economic Importance of Getting Data Protection Right: Protecting Privacy, Transmitting Data, Moving Commerce" (March 2013); available at https://www.uschamber.com/sites/default/files/documents/files/020508_EconomicImportance_Final_Revised_lr.pdf

Mr. ISSA. Thank you.
Mr. Black.

TESTIMONY OF ED BLACK, PRESIDENT & CEO, THE COMPUTER & COMMUNICATIONS INDUSTRY ASSOCIATION

Mr. BLACK. Mr. Chairman, Ranking Member, and Members of the Subcommittee, thank you for your focus on this important issue.

Mr. ISSA. I'm afraid now you're not quite loud enough.

Mr. BLACK. Thank you for your focus on this important issue. CCIA members and our industry are directly impacted by barriers to international data flow, as are many other industry sectors that utilize our services. CCIA members alone generate revenues in excess of $540 billion, and employ over 750,000 workers. International data flows are critical to U.S. economic interests. While the top Internet brands are American-based, the majority of their users are abroad. And increasingly, our most important exports are access to platforms and provision of services. Internet platforms uniquely empower businesses to participate in the global economy.

Small businesses in the U.S. would be the biggest winners if we can eliminate digital trade barriers. This is not a zero-sum game, but a win-win one. Global citizens and economies would also benefit if other governments eliminate digital trade barriers, which effectively lock their own citizens out of the 21st century economy.

U.S. policies have not adequately adapted to the new reality. We excel at the export of bits, but under current trade rules, countries can far more easily block bits than bananas. While TPP begins to make progress on digital trade, the situation worsens faster than U.S. policy can respond. We must do more. We should bring trade cases against countries who block bits.

Unless the trade system meaningfully responds to Internet trade barriers, our industries have little to gain from the trade agenda. Five issues must be prioritized: Internet blocking; forced localization; intermediary liability; balanced copyright; and data protection. TPP should make progress on blocking and forced localization, but the problem is worsening. A third of the world's 3 billion-plus Internet users live where social media or messaging apps have been blocked, and adoption of forced localization policies abroad keeps accelerating.

Sensible intermediary liability rules are essential. Internet businesses have thrived here because of carefully-crafted legal safe harbors, but foreign liability rules frequently favor domestic plaintiffs. Foreign courts often shoot the messenger when users express unfavorable views online about government, royalty, or national heroes. This has to change.

Particularly troubling is so-called EU right to be forgotten. European data regulators are prohibiting online services from simply linking to published news accounts about individuals. Some have even prohibited linking to stories that reported on these cases, and have even demanded removal of such links worldwide. If foreign officials punish U.S. companies, for pointing U.S. citizens to lawfully published news articles, we must stand up for free trade and free speech.

Another barrier for digital exports is unbalanced copyright. We have failed to export strong copyright limitations along with strong protections. Thus, we are seeing demands for snippet taxes to be paid for the privilege of quoting news. Such taxes on U.S. services subsidize foreign news publishers and violate international law. Since U.S. policy hasn't made them a priority, we're seeing such laws metastasize in Spain, Germany, and elsewhere.

Finally, data protection barriers are a problem. Recently, the EU Court of Justice, as my colleagues have mentioned, struck down the Safe Harbor framework. This has been used by thousands of U.S. companies to lawfully transfer data between Europe and the U.S. This decision forces thousands of businesses to find alternative tools to ensure they can lawfully transfer data from the EU. Current alternatives are costly, piecemeal, and difficult to implement for all companies, especially smaller ones. It is essential that a Safe Harbor framework be implemented promptly.

For the Internet to flourish as a tool for innovation, expression, and commerce, we must commit to showing that users worldwide continue to have confidence in the services of U.S. Internet companies. Passage of the U.S. Freedom Act was a step in the right direction, as will be the hoped-for passage of the Judicial Redress Act. Our domestic policies must also reinforce our own commitment to the free flow of data. For example, since cross-border access to competitive telecommunications is essential to facilitating the free flow of data, eliminating bottlenecks in U.S. telecom networks via proceedings, such as FCC's current special access reform review will enhance our global credibility.

In conclusion, our economy's future is intertwined with the Internet, but threats to Internet commerce proliferate. We must prioritize protecting this vital part of U.S. commerce. Thank you.

[The prepared statement of Mr. Black follows:]

Statement of

Ed Black

President & CEO

The Computer & Communications Industry Association

"International Data Flows: Promoting Digital Trade in the 21st Century"

Subcommittee on Courts, Intellectual Property, and the Internet

Committee on the Judiciary, U.S. House of Representatives

November 3, 2015

Chairman Goodlatte, Ranking Member Conyers, Subcommittee Chairman Issa, Ranking Member Collins, and Members of the Subcommittee, my name is Ed Black, President & CEO of the Computer & Communications Industry Association. We appreciate the committee's attention to the important matter of international data flows. CCIA represents large, medium and small companies in the high technology products and services sectors, including computer hardware and software, electronic commerce, telecommunications and Internet products and services. Many CCIA members are directly affected by barriers to international data flows, and many other industry sectors who depend on their services are indirectly harmed by the growing problem of digital trade barriers. There is a lot on the line here: CCIA members employ more than 750,000 workers and generate annual revenues in excess of $540 billion.[1]

The modern Internet is the cornerstone of cross-border trade in goods and services. Cross-border e-commerce is estimated to represent between 10 to 15 percent of total global e-commerce, and could grow from a 2014 figure of $80 billion to as high as $350 billion by 2025.[2] This trade is critical to U.S. economic interests. International markets are important growth opportunities;[3] while the top global Internet brands are made in America, the vast majority of their users are now outside the United States.[4] We are not talking only about the digital transmission of things that could be shipped physically, like digital media. Increasingly, the

[1] A list of CCIA members is available at https://www.ccianet.org/members.

[2] U.S. International Trade Comm'n, *Recent Trends in U.S. Services Trade: 2015 Annual Report*, May 2015, at 116, http://www.usitc.gov/publications/332/pub4526.pdf, (hereinafter "*Recent Trends in U.S. Services Trade*").

[3] U.S. International Trade Comm'n, *Digital Trade in the U.S. and Global Economies, Part 1* (July 2013), http://www.usitc.gov/publications/332/pub4415.pdf.

[4] Mary Meeker, *Internet Trends 2014*, May 28, 2014, at 130, http://www.kpcb.com/blog/2014-internet-trends. By way of specific example, Google's total international revenue was 39% of its overall sales in 2005, whereas today 56% of its revenue comes from overseas. *Compare* Press Release, Google, *Google Announces Fourth Quarter and Fiscal Year 2005 Results*, Jan. 31, 2006, https://investor.google.com/earnings/2005/Q4_google_earnings.html *with* Press Release, Google, *Google Announces Fourth Quarter and Fiscal Year 2014 Results*, Jan. 29, 2015, https://investor.google.com/earnings/2014/Q4_google_earnings.html. Similarly, 83% of Facebook's users lie outside of the U.S. and Canada, while fewer than 50% of Facebook users were international as of 2008. *Compare* Facebook Company Info, http://newsroom.fb.com/company-info/ *with* Miguel Helft, *Facebook Makes Headway Around the World*, N.Y. Times, July 7, 2010, http://www.nytimes.com/2010/07/08/technology/companies/08facebook.html.

most important aspects of our trade involve access to platforms and provision of services. Internet platforms and services not only export services to users abroad; they also empower small- and medium-sized U.S. businesses to participate in international trade like never before.[5] Small businesses and individual craftsmen can use platforms like eBay and Etsy to sell their wares globally without the need for an international presence. Data shows that small- and medium-sized businesses on eBay who focused on international markets grew 57% faster than their more domestic-focused counterparts.[6] Similarly, payment processors like PayPal and Google Wallet allow the same small firms to process payments globally, and global Internet advertising networks like those offered by Facebook, Twitter, Google, and Amazon allow these companies and individual sellers to target potential customers across borders. Thus, breaking down barriers to digital trade would also help small business exporters who rely on global Internet services. But to be clear, eliminating trade barriers isn't a zero-sum, "us-versus-them" issue. When governments impose digital trade barriers, they deny their own citizens crucial tools to advance their own economic welfare, and risk being left behind in the 21st-century economy. Breaking down these barriers would be a win-win outcome.

But to achieve this, we have to recognize that blocking or interfering with users' access to online platforms and services is no different then blockading a port, and we must respond accordingly.

Unfortunately, U.S. trade policies haven't adapted to the new reality. While trade policy has dramatically reduced barriers to trade in goods, the liberalization of trade in services has

---

[5] *See, e.g.*, Andreas Lendle *et al.*, *There Goes Gravity: How eBay Reduces Trade Costs*, World Bank Research Paper No. 6253, Oct. 2012, http://www-wds.worldbank.org/external/default/WDSContentServer/IW3P/IB/2012/10/25/000158349_20121025161729/Rendered/PDF/wps6253.pdf; McKinsey Global Institute, *Internet Matters: The Net's Sweeping Impact on Growth, Jobs and Prosperity*, *supra* note 11.

[6] Brian Bicron, *et al.*, *2015 US Small Business Global Growth Report*, eBay Public Policy Lab, 2015, at 11, https://www.ebaymainstreet.com/sites/default/files/2015-us-small-biz-global-growth-report_0.pdf.

lagged behind. Yet the United States is increasingly a services economy.[7] In fact, the United States is the largest global exporter of services, exporting $662 billion in 2013.[8] Recent data also shows continued growth in our services trade, with the United States' surplus in services trade growing 2.2 percent to $5 billion from 2013 to 2014.[9]

The result is one of our most important exports—Internet services—do not get the same protection as what we import from other countries. Today, countries can far more easily block bits than bananas at the border, and that's a huge problem when much of our exports are bits. This has to change.

To protect the global trading economy and to protect our economic interests, U.S. trade policy must modernize. We need to give top priority to barriers to Internet trade and impediments to Internet-enabled services. We need to start considering bringing trade disputes against countries who are blocking bits. If nations want to argue that giving their populace access to social media raises national security matters, we need to bring the most extreme claims to the WTO. If the modern trade system cannot meaningfully respond to the needs of the Internet sector, then that industry has little to gain from backing the trade agenda.

My testimony highlights principle obstacles to digital trade, including filtering, blocking, and localization mandates, onerous intermediary liability regimes, unbalanced intellectual property laws, and the recent developments regarding the U.S.-EU Safe Harbor Framework.

---

[7] Bureau of Labor Statistics, *Current Employment Statistics, Employees on nonfarm payrolls by industry sector and selected industry detail seasonally adjusted*, http://www.bls.gov/web/empsit/ceseeb1a.htm (last modified Oct. 2, 2015).

[8] World Trade Organization, *International Trade Statistics 2014* (2014), at 17, 28, https://www.wto.org/english/res_e/statis_e/its2014_e/its2014_e.pdf.

[9] *Recent Trends in U.S. Services Trade* at 32.

FILTERING AND BLOCKING

The most conspicuous barriers to digital trade are the outright filtering and blocking of U.S. Internet platforms and online content.[10] These are hardly isolated events. Some estimates predict that 38% of the world's 3 billion-plus Internet users live in countries where popular social media or messaging apps were blocked in the past year.[11] These practices have clear trade-distorting effects. For example, when a social media or video platform is blocked, it is not only harmful to the service and users in question; it also immediately affects content providers, advertisers, and small businesses using the service to find and interact with new and existing customers.

Censorship methods most often consist of network-level blocking and filtering achieved through state control of or influence over communications infrastructure. Known offenders include Afghanistan, Burma, China,[12] Cuba, Egypt, Guatemala, Indonesia, Iran,[13] Kazakhstan, North Korea, Pakistan,[14] Russia,[15] Saudi Arabia, Syria, Tunisia, Turkey,[16] Turkmenistan, the United Arab Emirates, Uzbekistan, and Vietnam.[17]

---

[10] Sanja Kelly *et al.*, *Freedom on the Net 2014: Tightening the Net: Governments Expand Online Controls*, Freedom House, 2014, https://freedomhouse.org/sites/default/files/resources/FOTN%202014%20Summary%20of%20Findings.pdf.

[11] Sanja Kelly *et al.*, *Freedom on the Net 2015: Privatizing Censorship, Eroding Privacy*, Freedom House, 2015, at 15, https://freedomhouse.org/sites/default/files/FH_FOTN_2015Report.pdf.

[12] *See* Matthew Schruers, Testimony before the U.S.-China Economic & Security Review Commission, *Commercial Espionage and Barriers to Digital Trade in China*, June 15, 2015 *at* http://www.uscc.gov/sites/default/files/Schruers%20Testimony.pdf; U.S. International Trade Commission, *Digital Trade in the U.S. and Global Economies, Part 2*, August 2014, at 98, http://www.usitc.gov/publications/332/pub4485.pdf (hereinafter "*Digital Trade in the U.S. and Global Economies, Part 2*"). In China alone, informal estimates suggest that this blocking has easily cost American firms billions of dollars as they are pushed out of the market. Julie Makinen, *Chinese censorship costing U.S. tech firms billions in revenue*, L.A. Times, Sep. 22, 2015, http://www.latimes.com/business/la-fi-china-tech-20150922-story.html.

[13] Lorenzo Franceschi-Bicchierai, *Iran Takes Aim at Google, Wikipedia in Latest Internet Censorship Effort*, Mashable, May 16, 2014, http://mashable.com/2014/05/16/iran-google-wikipedia/; Michelle Moghtader, *Iran expands 'smart Internet censorship*, Reuters, Dec. 26, 2014, http://www.reuters.com/article/2014/12/26/us-iran-internet-censorship-idUSKBN0K40SE20141226.

[14] Rob Crilly, *Pakistan threatens to ban Google unless it cleans up YouTube*, The Telegraph, June 11, 2013, http://www.telegraph.co.uk/news/worldnews/asia/pakistan/10112655/Pakistan-threatens-to-ban-Google-unless-it-cleans-up-YouTube.html; *See* Gibran Ashraf, *Facebook censored 54 posts for 'blasphemy' in Pakistan in second*

DATA AND INFRASTRUCTURE LOCALIZATION

Many countries abroad continue to show interest in implementing data localization policies, which include mandated server localization and data storage. Accelerated by the impact of the Snowden revelations, the number of countries imposing or considering data and infrastructure localization requirements has increased in recent years. Stated motivations for these policies include the desire to ensure domestic privacy protections, to protect against foreign espionage, to guarantee law enforcement access to personal data, and to promote local economic development, but at root these policies are inspired by protectionist instincts. These regulations are often vaguely construed, inadequately articulated and, therefore, nearly impossible to effectively implement.[18]

Yet even as tools of protectionism, which the global trade system was built to oppose, data localization policies are likely to hinder economic development, rather than promote

---

half of 2014, Express Tribune, Mar. 18, 2015, http://tribune.com.pk/story/855030/facebook-censored-54-posts-for-blasphemy-in-pakistan-in-second-half-of-2014/.

[15] Miriam Elder, *Censorship row over Russian internet blacklist*, Guardian, Nov. 12, 2012, http://www.theguardian.com/world/2012/nov/12/censorship-row-russian-internet-blacklist; Sanja Kelly *et al.*, *Freedom on the Net 2013*, Freedom House, Oct. 2013, at 592, http://freedomhouse.org/sites/default/files/resources/FOTN%202013_Full%20Report_0.pdf; Amar Toor, *Russia banned Wikipedia because it couldn't censor pages*, The Verge, Aug. 27, 2015, http://www.theverge.com/2015/8/27/9210475/russia-wikipedia-ban-censorship; Rob Price, *Reddit is now censoring posts and communities on a country-by-country basis*, Business Insider, Aug. 14, 2015, http://www.businessinsider.com/reddit-unbanned-russia-magic-mushrooms-germany-watchpeopledie-localised-censorship-2015-8.

[16] Joe Parkinson *et al.*, *Turkey's Erdogan: One of the World's Most Determined Internet Censors*, Wall St. J., May 2, 2014, http://online.wsj.com/articles/SB10001424052702304626304579505912518706936; Reporters Without Borders, *Turkey, Enemy of the Internet?*, Aug. 28, 2014, http://en.rsf.org/turquie-turkey-enemy-of-the-internet-28-08-2014,46856.html; Emre Peker, Joe Parkinson & Sam Schechner, *Google, Others Blast Turkey Over Internet Clampdown*, Wall St. J., Apr. 1, 2014, http://online.wsj.com/articles/SB10001424052702303978304579473190997035788; Zeynep Karataş, *Ongoing censorship blocks Kurdish, critical, data-based media during time of crisis*, Today's Zaman, Aug. 15, 2015, http://www.todayszaman.com/anasayfa_ongoing-censorship-blocks-kurdish-critical-data-based-media-during-time-of-crisis_396569.html.

[17] *Digital Trade in the U.S. and Global Economies, Part 2* at 98.

[18] *See* Anupam Chander & Uyen P. Le, Breaking the Web: Data Localization vs. the Global Internet, UC Davis Legal Studies Research Paper No. 378, Apr. 2014, http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2407858 (hereinafter "Chander & Le"); *see also Digital Trade in the U.S. and Global Economies, Part 2*.

domestic industry.[19] As the McKinsey Global Institute documented in 2011, 75% of the value of the Internet accrues to traditional, non-Internet centric businesses through productivity gains and easier access to foreign markets.[20] As a result, such policies will invariably harm global competitiveness.[21]

We have see such policies arise in countries including Russia,[22] India,[23] China,[24] France,[25] Germany,[26] Nigeria,[27] Indonesia,[28] and Vietnam,[29] among others.

---

[19] Leviathan Security Grp., *Quantifying the Costs of Forced Localization* (2015), http://static1.squarespace.com/static/556340ece4b0869396f21099/t/559dad76e4b0899d97726a8b/1436396918881/Quantifying+the+Cost+of+Forced+Localization.pdf.

[20] Matthieu Pélissié du Rausas *et al.*, McKinsey Global Institute, *Internet Matters: The Net's Sweeping Impact on Growth, Jobs and Prosperity* (2011), http://www.mckinsey.com/insights/high_tech_telecoms_internet/internet_matters.

[21] For example, foreign investment will likely decline. Given the high cost of constructing data centers, many companies will simply opt out of serving markets with onerous data localization requirements, especially small- and medium-sized businesses. In 2013, the average cost of data centers in Brazil and Chile were $60.3 million and $43 million, respectively. Loretta Chao & Paulo Trevisani, *Brazil Legislators Bear Down on Internet Bill Push for Data Localization*, Wall St. J., Nov. 13, 2013, http://online.wsj.com/articles/SB10001424052702304868404579194290325348688.

[22] Paul Sonne, *Russia Steps Up New Law to Control Foreign Internet Companies*, Wall St. J., Sept. 24, 2014, http://online.wsj.com/articles/russia-steps-up-new-law-to-control-foreign-internet-companies-1411574920; Sergei Blagov, *Russia Clarifies Looming Data Localization Law*, Bloomberg BNA, Aug. 10, 2015, http://www.bna.com/russia-clarifies-looming-n17179934521/; Matthias Bauer, Hosuk Lee-Makiyama, & Erik van der Marel, *Data Localisation in Russia: A Self-imposed Sanction* (European Centre for International Political Economy June 2015),http://ecipe.org/publications/data-localisation-russia-self-imposed-sanction/.

[23] Chander & Le at 16-19; *Avoiding NSA clutches: India to launch internal email policy for government communications*, RT, Oct. 31, 2013, http://rt.com/news/india-nsa-internal-email-994/; Thomas K. Thomas, *National Security Council proposes 3-pronged plan to protect Internet users*, Hindu Business Line, Feb. 13, 2014, http://www.thehindubusinessline.com/info-tech/national-security-council-proposes-3pronged-plan-to-protect-internet-users/article5685794.ece; Matthias Bauer *et al.*, *The Costs of Data Localisation: Friendly Fire on Economic Recovery*, ECIPE Occasional Paper No. 3/2014, http://www.ecipe.org/app/uploads/2014/12/OCC32014__1.pdf.

[24] U.S.-China Economic & Security Review Commission, *Red Cloud Rising: Cloud Computing in China*, Sept. 2013, revised Mar. 2014, at 5, http://origin.www.uscc.gov/sites/default/files/Research/DGI_Red%20Cloud%20Rising_2014.pdf; AmCham China, *Protecting Data Flows in the US-China Bilateral Investment Treaty*, Apr. 2015, at 4, http://www.amchamchina.org/policy-advocacy/policy-spotlight/data-localization; Gillian Wong, *China to Get Tough on Cybersecurity*, Wall St. J., July 9, 2015, http://www.wsj.com/articles/china-to-get-tough-on-cybersecurity-1436419416; Austin Ramzy, *What You Need to Know About China's Draft Cybersecurity Law*, N.Y. Times, July 9, 2015, http://sinosphere.blogs.nytimes.com/2015/07/09/what-you-need-to-know-about-chinas-draft-cybersecurity-law/.

[25] *Appel public à commentaires sur le référentiel d'exigences applicables aux prestataires de services sécurisés d'informatique en nuage*, Aug. 11, 2014, http://www.ssi.gouv.fr/actualite/appel-public-a-commentaires-sur-le-referentiel-dexigences-applicables-aux-prestataires-de-services-securises-dinformatique-en-nuage/; Chander & Le at 12-13.

INTERMEDIARY LIABILITY

CCIA has long argued that the failure to modernize liability rules abroad has increasingly contributed to U.S. Internet companies being held liable abroad for conduct that has long been construed as lawful in the Internet ecosystem. These penalties deter direct investment and market entry by Internet companies, and as a consequence deny local small- and medium-sized enterprises Internet-enabled access to the global marketplace. They similarly discourage investment in and growth of domestic startups.[30] We know that increasing liability on intermediaries decreases venture capital investments. While U.S. Internet businesses have thrived domestically under carefully crafted legal frameworks in U.S. law, like the Digital Millennium Copyright Act safe harbors and Section 230 of the Communications Decency Act, international asymmetries in liability rules frequently favor domestic plaintiffs.[31] U.S. exporters encounter unreasonably hostile liability rules in numerous countries abroad, including France,[32]

---

[26] Alison Smale, *Merkel Backs Plan to Keep European Data in Europe*, N.Y. Times, Feb. 16, 2014, http://www.nytimes.com/2014/02/17/world/europe/merkel-backs-plan-to-keep-european-data-in-europe.html; Michael Birnbaum, *Germany looks at keeping its Internet mail traffic inside its borders*, Wash. Post, Nov. 1, 2013, http://www.washingtonpost.com/world/europe/germany-looks-at-keeping-its-internet-e-mail-traffic-inside-its-borders/2013/10/31/981104fe-424f-11e3-a751-f032898f2dbc_story.html; Glyn Moody, *Germany's data retention bill requires metadata to be kept in the country*, Ars Technica UK, May 19, 2015, http://arstechnica.co.uk/tech-policy/2015/05/germanys-data-retention-bill-requires-metadata-to-be-kept-in-the-country/.

[27] U.S. Department of State, *Nigeria Investment Climate 2015*, May 2015, at 13, http://www.state.gov/documents/organization/241898.pdf

[28] Chander & Le at 19-20.

[29] *Id.* at 24.

[30] Matthew Le Merle *et al.*, *The Impact of U.S. Internet Copyright Regulations on Early-Stage Investment: A Quantitative Study*, Booz & Co. (2011), http://static1.squarespace.com/static/5481bc79e4b01e4bf3eeed80/t/54877560e4b0716e0e088e54/1418163552585/Impact-US-Internet-Copyright-Regulations-Early-Stage-Investment.pdf.

[31] For a general overview of these issues, *see* Ignacio Garrote Fernández-Diez, *Comparative Analysis on National Approaches to the Liability of Internet Intermediaries for Infringement of Copyright and Related Rights*, http://www.wipo.int/export/sites/www/copyright/en/doc/liability_of_internet_intermediaries_garrote.pdf (comparative analysis on national approaches to the liability of Internet intermediaries for infringement of copyright and related rights).

[32] Cour d'appel [C.A.] Paris, Feb. 4, 2011, *André Rau v. Google and Aufeminin.com*; Cour d'appel [C.A.] Paris, Jan. 14, 2011, *Google Inc. v. Bac Films, The Factory et al.*; Robert Andrews, *Google Fined In French Court For Not Stopping Video Copyright Abuse*, paidContent, Mar. 9, 2011, *at* http://paidcontent.org/2011/03/09/419-google-fined-in-french-court-for-not-stopping-video-copyright-abuse; Cour d'appel [C.A.] Paris, Sept. 3, 2010, *LVMH v. eBay*, (*aff'g* Commercial Court Paris June 30, 2008); Cour d'appel [C.A.] Reims, July 20, 2010, *Hermes v. eBay* (*aff'g* T.G.I. Troyes, June 4, 2008); *see, e.g.*, Tribunal de grande instance [T.G.I.] Paris, Nov. 14, 2011, *Olivier*

Germany,[33] Italy,[34] India,[35] Thailand,[36] Vietnam,[37] Estonia,[38] among others. Foreign courts are all too willing to "shoot the messenger" when foreign users express unfavorable views about the government, royalty, or national heroes, for example. This has to change. If U.S. services exporters are going to have meaningful access to foreign markets, we need to ensure that courts

---

Martinez v. Google and Prisma Presse; *Sarl Louis Feraud Int'l v. Viewfinder Inc.*, 489 F.3d 474 (2d Cir. 2007) (non-French site ordered to remove the photographs from New York servers or face penalties of 50,000 francs per day).

[33] Karin Matussek, *Google Loses German Copyright Cases Over Image-Search Previews*, Bloomberg, Oct. 13, 2008, http://www.bloomberg.com/apps/news?pid=newsarchive&sid=a_C1wVkCvPww (reversed on appeal); *See also* Hamburg Regional Court, Sept. 26, 2008, *Horn v. Google*, Partial Verdict, Ref. No. 308 O 42/06; Anna Zeiter, *German Supreme Court Finds eBay Liable for Actively Promoted Third Party Copyright Infringements*, Stanford Center for Internet & Society, Dec. 18, 2013, http://cyberlaw.stanford.edu/blog/2013/12/german-supreme-court-finds-ebay-liable-actively-promoted-third-party-copyright; LG Hamburg, Apr. 20, 2012, *GEMA v. YouTube*, Ref. No. 310 O 461/10; Karin Matussek, *Google's YouTube Must Help Detect Illegal Uploads, Court Says*, Bloomberg News, Apr. 20, 2012, http://www.businessweek.com/news/2012-04-20/google-s-youtube-must-help-detect-illegal-uploads-court-says.

[34] The Finocchiaro Law Firm, *Yahoo! Announces its intention to appeal against the order of the Court of Rome*, Apr. 13, 2011, http://www.blogstudiolegalefinocchiaro.com/wordpress/2011/04/yahoo-announces-its-intention-to-appeal-against-the-order-of-the-court-of-rome; Giulio Coraggio, *Yahoo! Liable for Searchable Contents!*, DLA Piper, IPT Italy, Apr. 3, 2011, http://blog.dlapiper.com/IPTitaly/entry/yahoo_liable_for_searchable_contents. *See also* Béatrice Martinet Farano, *Internet Intermediaries' Liability for Copyright and Trademark Infringement: Reconciling the EU and U.S. Approaches* 134 (Stanford-Vienna Transatlantic Tech. Law Forum (TTLF) Working Paper No. 14, 2012), *at* http://www.law.stanford.edu/sites/default/files/publication/300252/doc/slspublic/farano_wp14-4.pdf (noting that "most UGC [user-generated content] websites relying on an advertisement business models [sic] should be denied hosting protection" under recent court decisions).

[35] Rishabh Dara, *Intermediary Liability in India: Chilling Effects on Free Expression on the Internet* (2011), http://cis-india.org/internet-governance/intermediary-liability-in-india.pdf; Amol Sharma, *Facebook, Google to Stand Trial in India*, Wall St. J., Mar. 13, 2012, *at* http://online.wsj.com/article/SB10001424052702304537904577277263704300998.html; Amol Sharma, *In Search of Justice at the Google, Facebook Trial*, India Real Time, Mar. 13, 2012, *at* http://blogs.wsj.com/indiarealtime/2012/03/13/in-search-of-justice-at-the-google-facebook-trial.

[36] James Hookway, *Conviction in Thailand Worries Web Users*, Wall St. J., May 30, 2012, *at* http://online.wsj.com/article/SB10001424052702303674004577435373324265632.html (noting that this "sets a concerning precedent for prosecuting website owners for what their users say online."). *See also* Center for Democracy & Technology, *Comments on Thailand's Proposed Computer-Related Offenses Commission Act*, March 2012, *at* https://cdt.org/files/pdfs/Comments-Thailand-CCA-Draft.pdf; Jeremy Malcolm, *Intermediary Liability in Thailand Done Right and Done Wrong*, Electronic Frontier Foundation, Apr. 3, 2015, https://www.eff.org/deeplinks/2015/04/intermediary-liability-thailand-done-right-and-done-wrong.

[37] James Hookway, *Vietnam Rights Record Cools U.S. Ties*, Wall St. J., Aug. 8, 2013, *at* http://online.wsj.com/article/SB10001424127887323838204579000160962041046.html; Thuy Nguyen, *Online Intermediaries Case Studies Series: Roles and Liabilities of Online Intermediaries in Vietnam – Regulations in the Mixture of Hope and Fear*, The Global Network of Internet & Society Research Centers (2015) at 8, *at* http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2566364.

[38] Mark Scott, *Estonian News Site Can Be Held Liable for Defamatory Comments, Court Rules*, N.Y. Times, June 17, 2015, http://www.nytimes.com/2015/06/18/business/media/estonian-news-site-can-be-held-liable-for-defamatory-comments-court-rules.html; *see also* Heather Greenfield, *European Court Rules Online News Sites Liable For Online Comments*, CCIA News, Jun. 17, 2015, http://www.ccianet.org/2015/06/european-court-rules-online-news-sites-liable-for-online-comments/.

in those markets cannot penalize intermediaries for what third parties say on the Internet. This is particularly significant when the speech at issue would be protected by the First Amendment.

One particular aspect of this that deserves mention is European data regulators' enforcement of the so-called "right to be forgotten." Various courts have prohibited online services from linking to published news accounts about individuals, and in some cases even prohibited linking to stories that reported on court orders to disappear content.[39] It is problematic that courts might entertain an individual's desire to suppress their fellow citizens' access to media accounts of past criminality and corruption.[40] It is even more worrisome that some European data regulators have demanded the removal of such links *worldwide*.[41] When foreign officials threaten to fine U.S. companies for allowing U.S. citizens to read lawfully published media accounts, it is time to take a stand, not only for free trade, but free speech as well.

COPYRIGHT LIMITATIONS AND EXCEPTIONS

Balanced copyright rules such as fair use and related limitations and exceptions have been critical to the growth of the U.S. technology and Internet economy. We're increasingly finding that U.S. trade policy's failure to export strong limitations and exceptions along with strong copyright protections is hamstringing our businesses abroad and impeding U.S. exports.

For example, legislatures in Europe and elsewhere have increasingly proposed or implemented new publisher subsidies that are used against U.S. services, including social media,

---

[39] Daphne Keller, *Intermediary Liability and User Content Under Europe's New Data Protection Law*, Stanford Center for Internet & Society, Oct. 8, 2015, http://cyberlaw.stanford.edu/blog/2015/10/intermediary-liability-and-user-content-under-europe%E2%80%99s-new-data-protection-law; Samuel Gibbs, *Google ordered to remove links to 'right to be forgotten' removal stories*, Guardian, Aug. 20, 2015, http://www.theguardian.com/technology/2015/aug/20/google-ordered-to-remove-links-to-stories-aboutright-to-be-forgotten-removals.

[40] Jane Wakefield, *Politician and paedophile ask Google to 'be forgotten'*, BBC News, May 15, 2014, http://www.bbc.com/news/technology-27423527

[41] Samuel Gibbs, *French data regulator rejects Google's right-to-be-forgotten appeal*, Guardian, Sept. 21, 2015, http://www.theguardian.com/technology/2015/sep/21/french-google-right-to-be-forgotten-appeal.

news aggregation, and search providers. U.S. and other providers of online search, news aggregation, and social media platforms are compelled to pay for the "privilege" of quoting from news publications. This proposal is often referred to as a quotation or snippet tax. Restrictions on the quotation right violate international obligations, including Article 10(1) of the Berne Convention,[42] and the TRIPS Agreement.[43]

But because U.S. trade policy has not made balanced copyright a priority, policymakers across Europe, in national capitals and Brussels, have now taken interest in using imbalanced IP laws as a vehicle to tax services exported by American Internet companies and thereby subsidize local publishers.[44] At present, laws in Spain and Germany pose the most significant barriers to U.S. exporters.

Germany enacted a so-called ancillary copyright law (*Leistungsschutzrecht*) in August 2013, extending copyright protection to news snippets, *i.e.* small text excerpts in search results, notwithstanding international obligations that require free quotation.[45] The German statute expressly holds search engines liable for making available to the public snippets in search results, thereby creating direct liability for the automatic processes by which search results are generated. The German Copyright Arbitration Board recently suggested that if the length of such 'snippets' exceeds seven words (excluding 'keywords'), then search engines and other news

[42] Berne Convention for the Protection of Literary and Artistic Works, art. 10(1), amended Oct. 2, 1979.
[43] TRIPS Agreement, art. 9 ("Members shall comply with Articles 1 through 21 of the Berne Convention (1971)").
[44] *EU's Oettinger mulls levy on Google - Handelsblatt*, Reuters, Oct. 28, 2014, http://www.reuters.com/article/2014/10/28/eu-commission-oettinger-idUSL5N0SN34020141028; *Oettinger Floats Proposal for EU-wide 'Google-tax'*, EurActiv, Oct. 29, 2014, http://www.euractiv.com/sections/innovation-enterprise/oettinger-floats-proposal-eu-wide-google-tax-309568; *EU plant Urheberrechtsabgabe im Internet*, Handesblatt, Oct. 28, 2014, http://www.handelsblatt.com/politik/international/schutz-geistigen-eigentums-bis-2016-eu-plant-urheberrechtsabgabe-ini-internet/10900130.html ("... Wenn Google intellektuelle Werte aus der EU bezieht und damit arbeitet, dann kann die EU diese Werte schützen und von Google eine Abgabe dafür verlangen").
[45] *See generally* Special 301 Comments of CCIA, Dkt. No. USTR-2012-0022, filed Feb. 8, 2013, *at* http://www.ccianet.org/wp-content/uploads/library/CCIA%20Comments%20on%20Special%20301%20[2013].pdf.

aggregators should be liable for the "snippet tax"[46]—in short, U.S. services have to pay to quote more than 8 words. This is inconsistent with U.S. copyright norms, and more significantly for this discussion, Berne and TRIPS.[47]

Spain's recent IP reforms imposed a similar "snippet tax," which also subjects normal quotations to a tax. The Spanish approach actually prohibits news producers from waiving compensation rights, meaning that news publishers cannot opt out even if they want to. Faced with this measure, Google suspended its Google News service in the Spanish market. Like the German *Leistungsschutzrecht*, the Spanish IP revision not only undermines market access for U.S. companies and distorts established copyright law, but it also violates the EU and Spain's treaty and WTO commitments.[48]

If U.S. exporters of Internet services are going to enter crucial markets abroad, we need to ensure that the copyright law in those jurisdictions protects our businesses. So far, we have failed to do that.

U.S.-EU SAFE HARBOR

The economic importance of the free flow of data across borders is best demonstrated by the scale of the benefits derived from transatlantic digital trade. The transatlantic relationship between the United States and European Union is a significant component of both economies, as

---

[46] Jennifer Baker, *You want a 6% Google Tax? Get lost, German copyright bods told: Only snippets longer than seven words are chargeable*, The Register, Sept. 28, 2015, http://www.theregister.co.uk/2015/09/28/google_tax_6_pe_cent_germany_fails/.

[47] *See, e.g.*, *Faulkner Literary Rights v. Sony Pictures Classics*, 953 F. Supp. 2d 701 (N.D. Miss. 2013) (finding quotation of nine words to be non-infringing). *See also* CCIA White Paper, *Understanding 'Ancillary Copyright' in the Global Intellectual Property Environment*, at 5-6, *at* http://cdn.ccianet.org/wp-content/uploads/2015/02/CCIA-Understanding-Ancillary-Copyright.pdf (February 2015) (explaining Berne authors rejection of requirement that quotations be "short").

[48] *See* Raquel Xalabarder, *The Remunerated Statutory Limitation for News Aggregation and Search Engines Proposed by the Spanish Government - Its Compliance with International and EU Law*, IN3 Working Paper Series (Sept. 30, 2014), *at* http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2504596.

each is the other's largest market for goods and services.[49] Within that vital relationship, digital trade continues to increase in relative importance as digitally delivered services become more and more essential to overall economic activity. In 2012, the Brookings Institute estimated that U.S. exports of digitally deliverable services to the EU were worth $140.6 billion, or 72% of services exports, and the EU's share of digitally deliverable exports to the U.S. comprised 60% of services exports, amounting to $106.7 billion.[50]

However, recent developments have called into question the ongoing health of the transatlantic digital relationship. There are serious concerns about the continued viability of the EU-U.S. Safe Harbor Framework, which has been the primary mechanism enabling commercial data flows across the Atlantic over the last 15 years.[51] The Safe Harbor Framework has been historically used by more than 4,000 U.S. companies, along with the U.S. subsidiaries of EU companies, to lawfully transfer data about EU citizens from Europe to the United States in compliance with European data protection regulations.[52] In addition to being a direct contributor to the economic benefits that inure from transatlantic digital trade, the Safe Harbor has been a boon to transatlantic digital innovation. The efficiency gains from unimpeded cross-border data flows have enabled small businesses on both sides of the Atlantic to enter previously inaccessible markets and compete at scale. In fact, a full sixty percent of the companies who have certified

[49] *See* Joshua P. Meltzer, *The Importance of the Internet and Transatlantic Data Flows for U.S. and EU Trade and Investment* 4 (Brookings Institute, Global Economy & Development Working Paper No. 79, 2014), *at* http://www.brookings.edu/~/media/research/files/papers/2014/10/internet-transatlantic-data-flows-meltzer/internet-transatlantic-data-flows-version-2.pdf.

[50] *Id* at 12.

[51] Export.gov, *U.S.-EU Safe Harbor Overview*, http://export.gov/safeharbor/eu/eg_main_018476.asp (last visited Oct. 29, 2015).

[52] Department of Commerce International Trade Administration, *Key Points Concerning the Benefits, Oversight, and Enforcement of Safe Harbor*, *at* https://business.usa.gov/export-portal?static/Safe%20Harbor%20Key%20Points%2012-2013_1.atest_eg_main_068867.pdf.

compliance with the requirements of the Safe Harbor Framework are small- and medium-sized enterprises.[53]

Unfortunately, early last month in the *Schrems* case, the Court of Justice of the European Union (CJEU) ruled against the legal underpinnings of the EU-U.S. Safe Harbor Framework.[54] The *Schrems* case was brought in the wake of the first disclosures of widespread electronic surveillance by the United States' intelligence apparatus. The Court argued that the European Commission, in its original finding that the Safe Harbor was adequate under EU law, failed to appropriately weigh the national security and surveillance practices of the United States relative to the limitations and exceptions found in the Safe Harbor.[55] In particular, the Court focused on a lack of transparency, oversight, and legal remedies for European citizens.[56]

What does this decision mean for transatlantic data flows? In the near term, it means that the thousands of businesses—small and large—that have transferred data from Europe in compliance with the Safe Harbor will have to find alternative mechanisms to ensure that they can continue to do so in compliance with EU law. The currently available alternatives to permit EU-compliant data transfers are complex legal mechanisms, including binding corporate rules and standard contract clauses.[57] Both options are costly, piecemeal, time-consuming, and difficult to implement for even the most sophisticated companies. Expecting small- and medium-sized enterprises to successfully adopt these alternatives, particularly in the short term, to comply with the varying requirements of the data protection authorities of each EU member state would seem

---

[53] *Id.*

[54] Case C-362/14, *Maximillian Schrems v. Data Protection Commissioner*, Court of Justice of the European Union, http://curia.europa.eu/juris/document/document.jsf;jsessionid=9ea7d2dc30dd028f031e9795435bbb33d1623614d833.e34KaxiLc3qMb40Rch0SaxuRbN90?text=&docid=169195 (2015).

[55] *See id.*

[56] *See id.*

[57] *See* Press Release, Article 29 Working Party, Statement on Schrems Judgement (Oct. 16, 2015), *at* http://ec.europa.eu/justice/data-protection/article-29/press-material/press-release/art29_press_material/2015/20151016_wp29_statement_on_schrems_judgement.pdf.

unlikely. Moreover, these alternative mechanisms may also be called into question by future regulators, just as the Safe Harbor was.[58]

In the long term, the absence of a clear, reliable mechanism for lawful transfer of data across the Atlantic will lead to significant economic consequences. Larger companies may attempt to comply by building costly local facilities for processing and storage of data in the EU. Smaller firms may not be able to bear this burden, and could be forced to exit European markets. All told, in 2013 it was estimated that a serious disruption of this very kind to cross-border data flows with the EU would likely cost the EU between 0.8% and 1.3% of its GDP.[59] Those costs are likely to be considerably higher today—on both sides of the Atlantic.

Fortunately, a revised Safe Harbor Framework between the U.S. and the EU has been under negotiation by the Department of Commerce and European Commission since 2013 and is close to completion.[60] In the wake of the *Schrems* decision, it is important that the commitments in a new agreement be responsive to the concerns that the Court raised in their opinion. The new agreement must strike a delicate balance between the ongoing need for data-driven innovation to benefit consumers and small businesses and to drive economic growth, and a responsible, principles-based framework to ensure consumer protection. And most importantly, it must do so in a way that can be maintained in the long term, as legal certainty is a key ingredient for sustained transatlantic investment and growth in digital services. Where the revised agreement cannot be responsive to concerns of government access to data in the U.S. and the EU, national

[58] *See* Michelle Gyves, *German DPAs Announce Policy Severely Limiting Mechanisms for Lawful Germany-to-U.S. Data Transfers*, Proskauer Privacy Law Blog, Oct. 26, 2015, http://privacylaw.proskauer.com/2015/10/articles/european-union/german-dpas-announce-policy-severely-limiting-mechanisms-for-lawful-germany-to-u-s-data-transfers/.

[59] Matthias Bauer, *et al.*, *The Economic Importance of Getting Data Protection Right: Protecting Privacy, Transmitting Data, Moving Commerce*, ECIPE (2013), *at* https://www.uschamber.com/sites/default/files/documents/files/020508_EconomicImportance_Final_Revised_lr.pdf

[60] *See* Vera Jourová, European Commissioner for Justice, Consumers, and Gender Equality, Remarks on Safe Harbour EU Court of Justice judgement before the Committee on Civil Liberties, Justice and Home Affairs (Oct. 26, 2015), *at* http://europa.eu/rapid/press-release_SPEECH-15-5916_en.htm.

governments must work together to develop a lasting solution that ensures individual rights are appropriately balanced with targeted requests.

The uncertainty that companies now face with respect to continued transatlantic data flows is merely the most recent and acute result of the significant trust deficit that U.S. digital service providers have struggled to overcome in the wake of the last two years of disclosures about the United States' electronic surveillance programs. For the United States to continue to reap the substantial benefits of those data flows, it must take steps to rebuild the confidence of Internet users in Europe and worldwide.

I want to commend this Committee for the work it has already done in this regard. It led the way by being the first body to pass the USA Freedom Act earlier this year, and recently favorably reported the Judicial Redress Act, which then passed the House just two weeks ago. The USA Freedom Act contained a number of long-overdue oversight and transparency reforms to the electronic surveillance apparatus of the United States, while still preserving limited essential tools. The Judicial Redress Act would grant citizens of certain allied countries specific rights to ensure the accuracy and proper handling of their data[61]—rights that our own citizens already enjoy here and abroad. The Act's passage in the Senate is critical to the viability of future law enforcement and commercial data transfers. It is both a matter of basic fairness to reciprocally extend these rights, and a showing of good faith to allies and Internet users in Europe that we are committed to reasonable privacy standards with respect to data held by our government.

The lifeblood of our Internet-based industry—which today has grown to include a substantial component of all the United States' industries—is the trust that global Internet users have in online platforms. The private sector and government, both here and in the EU, must

[61] *See* Judicial Redress Act, H.R. 1428, 114th Cong. (2015).

work together to demonstrate to users worldwide that they should continue to place their confidence in the services of our Internet companies, which will in turn allow the Internet to flourish as a tool for innovation, expression, and commerce.

CONCLUSION

As the global Internet continues to grow and becomes even more tightly intertwined with international commerce, digital trade barriers will proliferate if left unchecked. To push back against these barriers, U.S. trade policy and enforcement priorities must be updated to reflect the growing significance of the Internet to the U.S. economy and U.S. trade performance.

Mr. ISSA. Thank you.
Mr. MacCarthy.

TESTIMONY OF MARK MacCARTHY, SENIOR VICE PRESIDENT, PUBLIC POLICY, SOFTWARE & INFORMATION INDUSTRY ASSOCIATION

Mr. MACCARTHY. Chairman Issa, Ranking Member Nadler——
Mr. ISSA. Once again, we'd like to hear you better.
Mr. MACCARTHY. Is that better?
Mr. ISSA. Pull it a little closer, and let's see.
Mr. MACCARTHY. Is that better?
Mr. ISSA. Yes. Sequestration gets us all.
Mr. MACCARTHY. On behalf of the technology trade association, thank you for your equipment.

I want to make a few points in my testimony. First, cross-border data flows fuel 21st century trade and investment across all sectors of the economy, not just technology or Internet companies.

Second, one goal of U.S. policy is to reduce barriers to trade—to traditional flows around the world. We should stay the course on this wise policy.

And third, the recent European decision on the Safe Harbor is a step backwards for open data flows. A new, workable, Safe Harbor must be put in place as soon as possible.

Mr. Chairman, digital trade involves tech products like software, where exports are growing at about 9 percent a year. But digital trade also involves business services generally, financial sector, royalties and licensing revenue, and communication services. It is 60 percent of all trade and services, it's growing three times faster than other service exports.

Digital trade increases our economic output by up to $711 billion a year. As Mr. Conyers mentioned, that's 4.8 percent of our gross domestic product, and it increases employment by 2.4 million workers. We have a global surplus in digital trade of $150 billion. A loss of open data flows would not be a minor sector-specific irritant. Data localization mandates have been studied for other economies. They would impose large welfare losses up to $63 billion for China, and $193 billion for the European Union.

Mr. Chairman, one goal of the U.S. trade policy is to promote cross-border data flows. Congress has instructed U.S. trade negotiators to dismantle measures that impede digital trade in goods and services that restrict cross-border data flows, or require a local storage or processing of data. Any exceptions have to be narrow, the least restrictive on trade and nondiscriminatory.

The United States has largely achieved these goals in the TPP agreement, although I concur with Ambassador Allgeier's remarks on financial services. That's an unfortunate exception, but we must seek similar outcomes in TTIP and TiSA.

Mr. Chairman, the demise of the Safe Harbor is a setback for open data flows. It has been in place since 2000, and the invalidation just this month left 4,400 companies in legal limbo, and that's not just technology companies. The list of Safe Harbor companies include many SIIA members, companies in online publishing and information services. In fact, the list of Safe Harbor companies reads like a Who's Who of American brand name corporations, in-

cluding Ford Motor Company, Starbucks, and the Walt Disney Company.

We need a new Safe Harbor. We need a Safe Harbor 2.0. Congress can help your passage of the Judicial Redress Act with a step forward. It's a modest step, but one that we need to follow in the Senate. We're hopeful that the Senate will act quickly on this bill and move forward with it.

Mr. Chairman, we urge this Committee to stay the course on promoting data flows and to help establish a new Safe Harbor for transatlantic data sharing. I stand ready to answer any questions you might have.

[The prepared statement of Mr. MacCarthy follows:]

Prepared Testimony of

Mark MacCarthy
Senior Vice President, Public Policy
Software & Information Industry Association

Before the

Subcommittee on Courts, Intellectual Property and the Internet

Of the

Committee on the Judiciary

United States House of Representatives

On

"International Data Flows: Promoting Digital Trade in the 21st Century

November 3, 2015

Mr. Chairman and Ranking Member, I am Mark MacCarthy, Senior Vice President for Public Policy for the Software & Information Industry Association (SIIA). Thank you for the opportunity to share our views on International Data Flows.

The Software & Information Industry Association (SIIA) is the principal trade association for the software and digital information industries. The more than 700 software companies, data and analytics firms, information service companies, and digital publishers that make up our membership serve nearly every segment of society including business, education, government, healthcare and consumers. As leaders in the global market for software and information products and services, they are drivers of innovation and economic strength—software alone contributes $425 billion to the U.S. economy and directly employs 2.5 million workers and supports millions of other jobs. For more visit the SIIA Policy Home Page.

I want to make three points in my testimony. The first is that cross border data flows fuel 21st Century trade and investment across all sectors of economic activity, affecting not just Internet companies but all enterprises and organizations that have come to rely on modern information and communications technology. Second, one goal of U.S. trade policy is to reduce unwarranted barriers to digital flows. We have achieved substantial success in the recently concluded Trans-Pacific Partnership Agreement, and can look forward to similar achievements in other trade negotiations such as the Trade in Services Agreement and the Transatlantic Trade and Investment Partnership. Third, the recent decision by the European Court of Justice to invalidate the U.S.-EU safe harbor arrangement for transatlantic data sharing is in tension with our trade objectives for reducing unnecessary barriers to digital trade. If a workable new safe harbor framework is not put in place soon, the transatlantic data flows that fuel the world's largest trading and investment relationship could be at risk.

Many of SIIA's 700 member companies use the now-invalidated safe harbor arrangement for their transatlantic data transfers. The loss of the Safe Harbor Framework as a legal basis for the transfer of personal information from Europe creates substantial legal uncertainty and has required them to begin a process of seeking alternative mechanisms for these transfers that is likely to be extended and expensive. Our immediate goals include the provision of a reasonable transition period and interim guidance by European regulators. Longer term, we need the legal certainty that can be provided by a modernized Safe Harbor Framework.

We are supportive of the Committee's inquiry into these matters and grateful for their support of our efforts and those by U.S. Administration officials to accomplish these goals.

Economic Benefits of Cross-Border Data Flows

Open digital trade is critical to U.S. tech industries, which are major contributors to job creation and economic growth. According to a recent report from the Software & Information Industry Association, about 12 percent of American software production is exported, totaling up to $57 billion in 2012. Moreover, exports of software and related services have grown by at least 9 percent each year since 2006—nearly 50 percent faster than all other U.S. exports. These exports helped fuel a steady increase in software employment, from 778,000 jobs in 1990 to 2.5 million in 2014.

And software jobs are good jobs. In fact, through the recent recession the average computer system design worker made $86,457 per year—three times as much as the average wage offered by the other four industries that also created large numbers of jobs during the downturn.

But digital trade is important for the broader economy as well. In 2011, the Global McKinsey Institute published a ground breaking study on the impact of the new information and communications technologies on growth and jobs.[1] Key findings were that the Internet contributes 34 percent to gross domestic product in the 13 countries studied. In the developed countries studied, it accounted for 21 percent of GDP growth over the most recent five-year period. It also found that most of the economic value created by the Internet falls outside of the technology sector, with 75 percent of the benefits captured by companies in more traditional industries, and it created 2.6 jobs for each lost to technology-related efficiencies.

This study was followed by a Commerce Department assessment of international trade in the business services, communications services, royalty and licensing flows, and financial services, where digital technologies are thought to play an important role in facilitating trade.[2] The study found that trade in these "digitally-enabled services" grew from 45 percent of all trade in services in 1998 to 61 percent in 2010, rising at a rate of 9 percent per year, while all other services grew at only 3 percent a year.

---

[1] McKinsey Global Institute. Internet Matters: The Net's Sweeping Impact on Growth, Jobs, and Prosperity, May 2011.

[2] Maria Borga and Jennifer Koncz-Bruner Trends in Digitally-Enabled Services, Bureau of Economic Analysis US. Department of Commerce

The Commerce Department updated this study for 2011, finding that:[3]

- The United States exported $357.4 billion in digitally-deliverable services. This represented over 60 percent of U.S. services exports and about 17 percent of total U.S. goods and services exports.
- The United States imported $221.9 billion in digitally-deliverable services. This represented 56 percent of U.S. services imports and about 8 percent of total U.S. goods and services imports.
- The United States had a digitally-deliverable services trade surplus of $135.5 billion.
- The total value of digitally-deliverable services in the supply chain of total U.S. goods and services exports was $627.8 billion, or about 34 percent of total export value.
- The majority of U.S. digitally-deliverable services exports went to Europe and to the Asia and Pacific region.
- Specifically, the United States exported the highest value of digitally-deliverable services to the United Kingdom, Canada, Ireland, and Japan. The highest values of digitally-deliverable imports came from the United Kingdom, Bermuda, Switzerland, and Canada.

In response to a Congressional request, the International Trade Commission conducted two studies on digital trade, documenting the size and economic importance of cross border data flows for the global economy. The first study[4] confirmed the growth of "digitally-enabled services" from from $282.1 billion in 2007 to $356.1 billion in 2011, with exports exceeding imports every year. In the second study[5], the ITC found that digital trade contributes to economic output by improving productivity and reducing trade costs. These efficiencies meant that digital trade increased U.S. GDP by up to $710.7 billion or 4.8 percent and increased employment by up to 2.4 million full time workers. The Commission also estimated that removing global digital trade barriers could raise U.S. GDP by up to $41.4 billion, or 0.3 percent.

---

[3] Jessica R. Nicholson and Ryan Noonan, "Digital Economy and Cross-Border Trade: The Value of Digitally deliverable Services", US Department of Commerce, Economics and Statistics Division Issue Brief # 01-14, January 27, 2014

[4] United States International Trade Commission, "Digital Trade in the U.S. and Global Economies, Part 1", Pub.4415, Investigation No.332-531, July 2013

[5] United States International Trade Commission, "Digital Trade in the U.S. and Global Economies, Part 2", Pub.4485, Investigation No.332-540, August 2014

A recent Brookings report found that cross-border data flows between the U.S. and Europe are the highest in the world.[6] They are 50 percent higher than data flows between the U.S. and Asia and almost double the data flows between the U.S. and Latin America. These data flows underpin many aspects of the transatlantic economic relationship.

- In 2012, the United States exported $140.6 billion in digitally-deliverable services to the European Union. That same year, the EU exported to the U.S. $106.7 billion worth of digitally-deliverable services.
- The U.S. and the EU are globally competitive exporters of digitally-deliverable services. In 2012, the EU trade surplus with the world in this category was 168 billion. The U.S. trade surplus was $150 billion.
- Today, almost 40% of data flows between the U.S. and EU are generated by commercial and research needs and these uses account for a majority of the growth in transatlantic traffic.
- The potential for data flow growth is strong as the Internet of Things increasingly grows. Given the EU's $125 billion trade surplus with the U.S. in goods, data flows originating from Europe will likely increase.

According to the Brookings Report, digital flows are important for investment as well as trade. Since 2000, Europe has attracted 56 percent of U.S. global investment and the United States receives 56.2 percent of global European investment. Much of this investment consists of U.S. subsidiaries and affiliates doing business in Europe and European subsidiaries operating in the United States. In 2011, U.S. foreign affiliates in Europe delivered $312 billion worth of digitally deliverable services and European businesses in the U.S. provided $215 billion worth of digitally deliverable services. Continued uninterrupted data flows are essential to maintaining economic integration of this size.

Recent studies from the European Centre for International Political Economy show that a loss of open data flows would not be a minor, sector-specific irritant. One study estimates that data localization mandates in Russia would reduce their GDP by 0.27 percent, even taking into account possible positive economic benefits of local data storage.

Another study from ECIPE estimates that recently proposed or enacted data localization measures would reduced GDP by 0.2% in Brazil, 1.1% in China, 0.4% in the EU, 0.1% in India, 0.5% in Indonesia, 0.4% in Korea and 1.7% in Vietnam.

[6] Joshua Meltzer, The Importance of the Internet and Transatlantic Data Flows for U.S. and E.U Trade and Investment, Brookings Global Economy and Development Working Paper 79, October 2014

Actual economic losses by the citizens amount to up to $63 billion for China and $193 billion for the EU. For India, the loss per worker is equivalent to 11% of the average month salary, and almost 13 percent in China and around 20% in Korea and Brazil

It is sometimes thought that digital flows and trade benefit the exporting country more than the importing country. In this view, a strategy of digital protectionism can be seen as economically rational. But digital flows and trade improve economic performance in importing countries in a number of ways:

- Domestic productivity increases when firms are able to import the best computing and information services at the lowest prices.
- Online information services, Internet-based services, and computer services supply strategically important inputs for all sectors, goods, and services.
- A country that wants to excel in the provision of banking and financial services, education, tourism, construction, and healthcare services needs to allow its businesses and citizens to obtain the best possible inputs from information and computer service providers regardless of location.
- Worldwide suppliers of online and computer services provide the spur of competition to ensure that all service sectors excel. These suppliers help domestic exporting and manufacturing companies.
- Having a seamless flow of information and a flexible location of servers leads to increased price competition, better quality, and wider choice for consumers.
- Lower prices and a wider availability of information services and computer services lead to greater product and process innovation throughout a domestic economy.
- Lowering digital barriers would provide producers, investors, workers, and users with a clear idea of the rules of the game, thereby encouraging long-term investment and commitment to local markets.

U.S. Trade Policy on Cross-Border Data Flows

In principle, trade in digitally-enabled services is addressed in the General Agreement on Trade in Services (GATS). This multilateral trade agreement, signed in 1994 at the same time as the establishment of the World Trade Organization, commits signatory nations to reduce barriers to trade in service and to treat international service suppliers in the same way it treats its domestic service providers.

However, GATS is limited in several respects as a tool for enforcing open digital flows. Signatory nations are committed to open a particular service only if they have specifically agreed to do so. This creates a nightmarish complexity in determining which services are really open, a difficulty that is even greater since many of the key digital services did not exist in 1994 when the treaty was signed.

Moreover, under the general exceptions provided for in Article 14, even countries who have committed to a market opening measure in a particular service are permitted to adopt or enforce measures necessary to secure compliance with consumer protection laws and laws or regulations related to "the protection of the privacy of individuals in relation to the processing and dissemination of personal data and the protection of confidentiality of individual records and accounts."[7]

These privacy and consumer protection measures cannot be applied in a discriminatory manner or as "a disguised restriction on trade in services." But still this general exception can serve as a way for countries to step back from full commitment to open data policies, if they want to do so.

As a result, U.S. trade policy has sought to establish more explicit principles of openness in digital trade. A good start was made in the U.S. Korea Free Trade Agreement, but the text in the electronic commerce chapter was hortatory, requiring the signatories merely to "endeavor to refrain from imposing or maintaining unnecessary barriers to electronic information flows across borders."

In the Trans-Pacific Partnership negotiations, the U.S. sought binding commitments for cross-border data flows. In particular, USTR sought "requirements that support a single, global Internet, including ensuring cross-border data flows, consistent with governments' legitimate interest in regulating for purposes of privacy protection…(and)…rules against localization requirements that force businesses to place computer infrastructure in each market in which they seek to operate, rather than allowing them to offer services from network centers that make business sense."[8]

In 2011, USTR succeeded in negotiating an agreement with Europe that contained prohibitions on data and server location.[9] One provision provided that

---

[7] Article XIV, General Agreement on Trade in Services at https://www.wto.org/english/docs_e/legal_e/26-gats_01_e.htm

[8] USTR, Trans-Pacific Partnership: Summary of U.S. Objectives https://ustr.gov/tpp/Summary-of-US-objectives

[9] USTR, United States-European Union Trade Principles For Information and Communication Technology Services, April 2011 at http://trade.ec.europa.eu/doclib/docs/2011/april/tradoc_147780.pdf

"governments should not prevent service suppliers of other countries, or customers of those suppliers, from electronically transferring information internally or across borders, accessing publicly available information, or accessing their own information stored in other countries." Another provision said, "Governments should not require ICT service suppliers to use local infrastructure, or establish a local presence, as a condition of supplying services."

Congress approved these policy initiatives on cross-border data flows in trade promotion authority legislation. One provision of the law is a directive to U.S. trade negotiators "to ensure that governments refrain from implementing trade-related measures that impede digital trade in goods and services, restrict cross-border data flows, or require local storage or processing of data."

The trade promotion authority law also address the concern that domestic policy objectives might sometimes affect digital trade, specifying that U.S. policy on this point is that such exceptions needed to be narrow: "where legitimate policy objectives require domestic regulations that affect digital trade in goods and services or cross-border data flows, to obtain commitments that any such regulations are the least restrictive on trade, nondiscriminatory, and transparent, and promote an open market environment."

The United States has largely achieved these negotiating goals in the recently concluded Trans-Pacific Partnership (TPP) Agreement. According to the USTR:

"In the Electronic Commerce chapter, TPP Parties commit to ensuring free flow of the global information and data that drive the Internet and the digital economy, subject to legitimate public policy objectives such as personal information protection. The 12 Parties also agree not to require that TPP companies build data centers to store data as a condition for operating in a TPP market..."[10]

SIIA is strongly supportive of this development. Clearly, given the importance of data flows for modern economies, the United States must seek similar outcomes in the Transatlantic Trade and Investment Partnership (T-TIP) negotiations.

For the TTIP negotiations, USTR has already set out cross border data flow objectives, seeking to "include provisions that facilitate the movement of cross-border data flows" on the grounds that "free flows of data are a critical component

[10] USTR, Summary of the Trans-Pacific Partnership Agreement at https://ustr.gov/about-us/policy-offices/press-office/press-releases/2015/october/summary-trans-pacific-partnership

of the business model for service and manufacturing enterprises in the U.S. and the EU and key to their competitiveness."[11]

The Trade in Service Agreement (TISA) will also consider cross border trade in services and data flows. Recently, SIIA held a discussion for the TISA negotiators and others in Geneva focused on the data flows and discussing ways in which countries could have both strong privacy rules and modern data flows.[12]

The European Court of Justice Invalidation of the Current Safe Harbor Data Sharing Arrangement

The European Data Protection Directive of 1995 prohibits commercial data transfers abroad unless the country to which the data is being sent has an "adequate" level of data protection.[13] In 2000, the European Commission ruled that company adherence to a set of negotiated privacy practices would be adequate for data transfers to the United States.[14] These privacy practices include notice, choice, onward transfer, access, security, data integrity and enforcement. Companies self-certify that they follow these practices and their name is published at a Department of Commerce website.[15] Their promise to follow these practices is enforceable by the Federal Trade Commission, which has taken 10 enforcement actions from 2009 to 2013 and has stepped up enforcement substantially since then.[16]

This Safe Harbor Framework has provided a convenient and effective legal basis for U.S companies and subsidiaries of European companies to comply with European regulations on commercial data transfers, which typically include data

[11] USTR, T-TIP Issue by Issue Information Center at https://ustr.gov/trade-agreements/free-trade-agreements/transatlantic-trade-and-investment-partnership-t-tip/t-tip-15

[12] Software & Information Industry Association, The Cross-Border Data Flow Discussion Comes to Geneva, at http://blog.siia.net/index.php/2015/10/the-cross-border-data-flow-discussion-comes-to-geneva/

[13] European Data Protection Directive 1995 at http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52012PC0010

[14] European Commission, Commission Decision of 26 July 2000 pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequacy of the protection provided by the safe harbour privacy principles and related frequently asked questions issued by the US Department of Commerce at http://eur-lex.europa.eu/legal-content/en/ALL/?uri=CELEX:32000D0520

[15] U.S. Department of Commerce, Welcome to the EU – US Safe Harbor Framework at http://www.export.gov/safeharbor/

[16] Future of Privacy Forum, The US EU Safe Harbor, December 2013 at http://www.futureofprivacy.org/wp-content/uploads/FPF-Safe-Harbor-Report.pdf

from employees, such as payroll information, and information about a company's European customers, suppliers, vendors, and partners.

Two years ago, to help restore public trust in the aftermath of revelations about U.S. surveillance activities, the European Union and the United States began negotiations for a modernized commercial data sharing arrangement.

On October 6, however, just as these discussions were coming to a conclusion, the European Court of Justice issued a ruling that invalidated the existing Safe Harbor on the grounds that U.S. privacy protections relating to mass surveillance of European citizens were not adequate.

Suddenly, the roughly 4,400 European and U.S. companies that have been using the Safe Harbor were thrown into a kind of legal limbo. After a meeting on October 16, the European data protection regulators said that other legal bases for transfers are still available including model contractual clauses and binding corporate rules. But moving to these alternatives cannot be done quickly or easily. In some cases, thousands of existing contracts have to be renegotiated.

The European regulators as a group urged EU negotiators to reach a new modernized safe harbor agreement with the United States by the end of January 2016. After which, they felt obliged to consider enforcement actions.

Some individual regulatory authorities, however, announced that they are considering enforcement proceedings even earlier than January. One data protection officer authority suggested to a magazine that companies might want to "consider storing personal data only on servers within the European Union."

European Commissioners in charge of negotiations have publicly said that they are close to a final agreement in principle on the new framework, a message echoed by U.S. Commerce Department officials. Passage of the Judicial Redress Act, they say, will facilitate the negotiation of a new safe harbor that will pass European court review.

On October 20, the House of Representatives passed the Judicial Redress Act by a voice vote. The House leadership, House Judiciary Chairman Bob Goodlatte, Ranking Member John Conyers, and Representative Jim Sensenbrenner all joined forces in a show of bi-partisan support for this vital legislation.

The legislation, which is supported by U.S. law enforcement and a broad industry coalition, is narrowly targeted to allow citizens of European nations and other designated allies the ability to request corrections of inaccuracies in data held by a number of U.S. agencies, verify their data has not been improperly disclosed, and

seek civil judicial recourse in certain circumstances. It is a modest step toward giving citizens in other countries procedural privacy protections similar to – but not exceeding - those available to U.S. citizens.

In passing the Judicial Redress Act, the House acted to advance U.S. international interests in globally effective law enforcement and the free flow of data across borders. The leadership of the Senate and the Senate Judiciary Committee should act quickly to pass the Senate version the legislation co-sponsored by Senators Chris Murray and Orrin Hatch.

The perception that the Safe Harbor is of use only or primarily for technology companies is false. Many of the online publishing and information service companies in SIIA use the Safe Harbor as well. The list of Safe Harbor companies reads like a who's who of American brand name corporations including Ford Motor Company, Starbucks and the Walt Disney Company.

The perception that the Safe Harbor is important only for U.S. companies is also false. Over 150 subsidiaries of European companies use the Safe Harbor, including well-known brands like Adidas, BMW, Bayer, Ericsson, Nokia, Bertelsmann, and Vodafone.[17] The demise of the Safe Harbor is bad news for these European companies.

Conclusion

Cross-border data flows are an intrinsic feature of the 21st century global information economy, as essential to today's economic, social, and political activity as air travel and electricity. Studies assessing the economic importance of data flows all agree that their benefits for growth, jobs and inclusive prosperity are large and growing. Conversely, attempts to turn back the technological tide through server or data localization requirements will impose tangible economic costs on the lives and economic activity throughout society.

The Congress has endorsed U.S. objectives to negotiate reasonable cross-border data provisions in trade agreements, including the successful outcome in the Trans-Pacific Partnership Agreement and the upcoming efforts in the Trans-Atlantic Trade and Investment Partnership and the Trade in Service Agreement. We urge this Committee to work with the Administration to stay the course.

[17] Future of Privacy Forum, EU-US Safe Harbor Essential To Leading European Companies at http://www.futureofprivacy.org/2014/04/30/eu-us-safe-harbor-essential-to-leading-european-companies/

The invalidation of the safe harbor transatlantic data sharing agreement is a set back. A failure to establish a modernized transatlantic data sharing agreement would be in some tension with the digital trade principles that the U.S. is seeking to implement in international trade agreements. It would greatly complicate negotiations on the upcoming TISA and TTIP trade agreements. It would be a step back from the openness of the past which allowed U.S. companies a convenient, effective and enforceable method to engage in cross border data flows while demonstrating compliance with data protection rules. A new data sharing arrangement is urgently needed to ensure that the transatlantic digital trade market stays as open and free as it has in the past.

Mr. ISSA. Thank you.

With that, Mr. Nadler has responsibility on the floor with his votes, so he will do the round of questioning, and then we will recess until after three quick votes.

Mr. NADLER. Thank you, Mr. Chairman.

Dr. Atkinson, in your testimony, you urge the U.S. to lead on reform of government access to data, so that other Nations do not have an excuse to restrict cross-border data flows. You also note that after the Edward Snowden revelations about the U.S. Government's expansive intrusive surveillance programs, a number of countries pulled data out of the U.S., and imposed restrictions on the flow of data to this country.

Can you describe the impact that the Snowden revelations had on American companies? And can you expand on what sorts of reforms we should put in place, if we lead on reform, as I agree we must?

Mr. ATKINSON. Sure. Thank you.

For a long time, countries were wanting to do these kinds of things, but never had the sort of public excuse or rationale. And a case in point is China. China, in the last year and a half, as I document in my testimony, has put in place a number of restrictive policies that negatively affect U.S. companies. And the goal there—and the reason they say they are doing it is because exactly because of the Snowden revelation. They talk about secure and controllable technology and other kinds.

And these are, just frankly, just an outright guise on their part. This is a policy they've long wanted to do to punish, or to favor their own domestic companies at the expense of U.S. companies. We see that in Germany, for example, where you have some major German technology companies that are marketing themselves as NSA free, and pushing the European Commission to adopt policies like the, quote, "European cloud," so that NSA or other law enforcement agencies in the U.S. couldn't get access to the data.

And there have been a number of cases that have been documented where U.S. technology companies have actually lost market share. We see that in Australia, where one of the leading cloud providers, domestic cloud providers in Australia, has been arguing the exact same thing; in fact, funding a report, trying to convince the Australian Government to ban storage of data outside the country with U.S. providers.

So in our view, it has been a systemic effort to target the leadership of U.S. technology companies. And what do we do about it? As I said, I really—I think it's a two-part process. It is that we do need—there are some reforms that we need to make domestically, a number of people talk about judicial redress, other steps that we could take. But at the same time, I would agree with a couple of other panelists who said I think we just have to get tougher on trade enforcement and negotiations with these countries, particularly China, which is getting away with murder on many, many fronts engaged in a systemic effort to take market share away from U.S. companies.

Mr. NADLER. Thank you. And as you know, FBI Director Comey and other law enforcement officials have argued that the government must maintain a backdoor into technology, and have opposed

strong encryption measures. Do you think that would be a mistake? And if so, why?

Mr. ATKINSON. I do think that's a mistake. I think it's a mistake for several reasons: Number one, if the technology is inextricably going in the direction of unbreakables, encryption where the key is not public, it's just between two parties, the technology provider doesn't have the key, the government doesn't have the key, that's where the technology is going. I think the FBI is fighting a losing battle there, as they fought a losing battle in the '90's with the clipper chip.

The second problem with that is if they mandate—try to mandate that, they are setting, I think, a dangerous precedent, for example, by letting the Chinese Government do the exact same thing. The Chinese Government is trying to do the same thing right now to prevent encryption in China for U.S. companies.

And, finally, weakening our encryption technology that U.S. companies would use, why give the FBI more access? We would also give the Chinese and the Russians and anybody else who wants to do harm to us, it would give them access as well.

Mr. NADLER. Thank you. My last question to you, and I think for this series is, as you explained in your testimony, support for free trade and data does not mean we must allow the free flow of illegal content like child pornography or email stem or pirate creations and other banned products. But what if two countries have different standards of what is illegal or objectionable? You may have a country that thinks political dissent is objectionable, but pirated movies are perfectly acceptable. Even in a less extreme case, countries may treat certain content differently under the law. How should countries determine what data should be permitted to flow freely between them in cases of disagreement on these standards?

Mr. ATKINSON. Because, as I said earlier, I think it's an un—essentially, an untenable project that we would end up with global harmony on every single rule with regard to the Internet. We're not going to be able to do that. And we're certainly not going to be able to do that with free speech. There are certain countries, particularly more traditional, religious countries that find pornography objectionable. We dealt with our—at least we have free speech, we might found objectionable, but we allow it. We are not going to be able to agree on that. And for certain things like that, countries are going to do that, and I think we are just going to have to be okay with that.

Another example was in Germany, you're not allowed to download a copy of Mein Kampf. In the U.S., we can. Again, we're not going to change the German view. I don't know whether they are right or wrong, it doesn't make any difference. Where we can and should, though, take action is there are certain things that are clearly illegal under the WT0 framework for intellectual property.

For example, piracy and intellectual property, thus, can be prosecuted. So when countries engaged in steps, for example, to block certain Web sites that are clear piracy sites, like, for example, a domain called the Pirate Bay, that should be quite—you know, we should be encouraging that. That's quite different than blocking, say, you know, Facebook or something like that, or blocking some site just because you don't want competition.

I think the key step, though, is we have to understand, just in free trade—in good free trade, there's certain things that we don't allow trade in. Like elephant ivory, we signed a global agreement, we shouldn't trade in that. It doesn't mean we don't support free trade. I would argue we should apply the same standards, things like malware or a pirated content and the like.

Mr. NADLER. Thank you very much.

Mr. ISSA. I thank all of you. We're going to—we'll stand in recess until 5 minutes after the last of 3 votes begin, because I will vote, and I will walk. So 5 minutes after that, I will be here, and we will pick up with those who are present.

We stand in recess.

[Recess].

Mr. ISSA. The Committee will come to order. I'll now recognize myself for my 5 minutes or longer, if people doddle getting back.

Ambassador, when you talked about—I believe you talked about the carveout for banks. Can you go through one thing with me? What could possibly prompt the United States Government to want to carve out banks?

Mr. ALLGEIER. Well, our understanding, from having met with various agencies in the U.S. Government, is that the Treasury Department wants to maintain the flexibility that sometime in the future, it might want to impose a localization requirement. We do not understand that because the issue is, will data be made available for prudential reasons, security, for law enforcement. And in this world, it doesn't matter where the data is. You can get it instantaneously, as you know.

Mr. ISSA. Well, let me ask you a rhetorical question: Localization versus duplication. If the United States Government had said that on all American persons and/or all accounts, whether owned by non-U.S. persons or U.S. persons, there must be maintained a copy in the United States, thus not requiring localization but simply the ability to get a copy related to U.S. bank accounts, wouldn't that have met all of their requirements?

Mr. ALLGEIER. Well, that certainly does add an element of additional cost to the operation, and so in that sense, they're not happy—wouldn't be happy about that.

Mr. ISSA. Well, I hear you, but I want to have a dialogue for a moment, because I think part of the data question for all of us is cost. I hear you say cost, but in the—with the possible exception of the IRS, it doesn't seem they'll maintain 6 weeks of backups. In the ordinary course, backups are a relatively cheap mass storage.

So, again, the question I have for you is, regardless of where live data is hosted, realistically, the only American interest, the only U.S. interest was, for purposes of the IRS, 7 years worth of data, right? So let me ask again, wouldn't any country, for purposes of sufficient information to allow them to make the appropriate tracking for tax purposes, either demand that it be maintained, a copy be maintained where they could reach it by a U.S. law enforcement agency, or an agreement that would allow a long-arm relationship?

So, for example, if you're going to host in Britain, Germany, somewhere, there has to be an ability for the IRS to be able to ask for and receive that. Would that be an example—as a former trade ambassador, would that be an example of these carveouts that you

think are limited but appropriate as long as you can demonstrate the need, the specific need that is being preserved?

Mr. ALLGEIER. Well, certainly, it is an improvement in the sense that it's limited. But I guess the question again I say is, first of all, these businesses, insurance and banking, are highly regulated. If they don't provide the data, they can lose their license, and so——

Mr. ISSA. Okay. You've made my case in a sense. Isn't it true that without the U.S. having imposed this, they already had other requirements, the FDIC, and so on, that would have required banks and other financial institutions for various reasons to have a copy available for their observation and review, right?

Mr. ALLGEIER. Well, they have to make it available. The question is if the server is in Singapore and the IRS or the Fed or anybody else comes and says I want this data, how long does it take them to get it from Singapore? It doesn't take them any faster——

Mr. ISSA. It depends on the bandwidth of the pipe.

Mr. MacCarthy.

Mr. MACCARTHY. Mr. Chairman, I used to work at Visa, the payment card company, and so I'm familiar with how——

Mr. ISSA. Visa? Payment card?

Mr. MACCARTHY. Yeah.

Mr. ISSA. Small company. Okay.

Mr. MACCARTHY. Small company.

Mr. ISSA. I've heard of it.

Mr. MACCARTHY. I left there in 2008, but before that, we were familiar with the rules that the Federal regulators had in place, and they actually provided for outsourcing of bank records, and they had rules and guidance for how it should be done, making sure that U.S. law followed the records. And under existing case law, they have a full authority to reach out wherever the bank records are stored, and have the bank produce them for——

Mr. ISSA. So your position is that the United States asking for this in the trade agreement was unnecessary and counterproductive?

Mr. MACCARTHY. Unnecessary, counterproductive, and——

Mr. ISSA. Is there anyone that disagrees with it being unnecessary and counterproductive? Okay. Then we'll consider that it was unnecessary, counterproductive.

I'll close—because I want to get to the other folks that are now coming back—with a very simple question: To the best of your knowledge—and, you know, Mr. Snowden helped us have some of this knowledge, but—and WikiLeaks did, too, for that matter—isn't it true, that, for example, Nigeria, a country that loses half a billion dollars a month of oil, which is tangible and hard to steal, is, in fact, a place where if the United States wanted to get any and all records hosted there, they would be able to do so easier in Nigeria, and be able to do so without the court's supervision at all? Because ultimately, once something leaves the United States, the United States is under no obligation not to—the NSA, which has been mentioned here previously, can simply take what they want, assuming they have the technology.

Isn't that true that the countries who demand that the data be kept in their country and out of the U.S. actually lose protection

that is granted in the United States for under the Fourth and other amendments?

Okay. We'll assume that I knew the answer to that one. Ms. Espinel?

Ms. ESPINEL. I was just going to point out that there is a certain irony in a country like Nigeria, which is one of the countries that's putting in place things like data localization laws.

Mr. ISSA. I used them because they can't even keep track of their own oil.

Ms. ESPINEL. When I think the processes that we have in the United States to protect due processes and civil liberties. I think our system would stand up well against their system. So Nigerial is one of the countries of the concern, and there is a certain irony there.

Mr. ISSA. But let me do a final, and it's a rhetorical question, but isn't it true, really, that Nigeria hosting their Nigerian information really simply means that, like China and other countries, they have the ability to take, without due process potentially, the information of their citizens where if it's hosted in the U.S., there would be due process?

Yes, Dr. Atkinson.

Mr. ATKINSON. I completely agree with that. There are a lot of countries that have nowhere near the due process, the rule of law that we have, and in that sense, data stored in those countries can be quite problematic. That's why I raised my earlier point about the European Commission cutting us off in the Safe Harbor, but leaving in some other countries that have at least the same, if not more dubious protections for government access to data.

Mr. ISSA. Thank you. And I look forward to additional questions.

And with that, I'd like to go to the Ranking Member of the full Committee, the gentleman from Michigan, Mr. Conyers.

Mr. CONYERS. Thank you, Mr. Chairman.

I am struck by the unanimity among the five witnesses today, and I commend them all.

Let me start with Dr. Atkinson. And keeping in mind the privacy concerns of Americans and our allies, how can the United States and its trade partners move forward to advance free data trade? And I understand you have some regrets about strong encryption.

Mr. ATKINSON. Is the question—I'm sorry—about encryption? Is that——

Mr. CONYERS. No. It's how they advance free data trade. That's the main idea here in this question.

Mr. ATKINSON. Well, I think the challenge is that countries will use the guise of privacy as an excuse for protectionism. And as I—I think the Chairman's comment—question alluded to this, I think, central point, which is, as long as countries—as long as companies have nexus in a country, if they're doing business in a country, they cannot get out from under that country's privacy and commercial security rules and laws by moving data to a third country.

They still have to comply with those laws no matter where the data are located. And I think that's really the fundamental principle that we have to go by with this. So you can protect—you could have—you can protect the privacy of your citizens, and you don't

have to require the data be located there, as long as you have jurisdiction over the company doing business there.

Mr. CONYERS. Thank you.

Mr. Allgeier, with regards to privacy, what's been done, and what do you think still needs to be done in order to ensure the viability of cross-border data flows?

Mr. ALLGEIER. Well, there is a structure in place already in the WTO, the World Trade Organization, and the agreement there on trade and services. And what it says explicitly is that governments may put in various restrictions on data to achieve certain ends.

And one of them, specifically, is to protect the privacy of individuals in the processing and dissemination of personal data. And so, all of the countries are obliged to recognize that. And so, if a country does put in place certain privacy rules, that's legitimate.

Mr. CONYERS. Absolutely.

Now, we passed the Judicial Redress Act. We are hoping that the other body will act with appropriate swiftness. But I think we may have something else to think about.

Mr. MacCarthy, can you elaborate on how the Judicial Redress Act affects the companies that you represent?

Mr. MACCARTHY. Thank you for that question. The Act doesn't directly affect our companies. What it does do is to create a reason for the European negotiators in Safe Harbor to move ahead with finalizing the agreement. And when the agreement is finalized, then it would create enormous benefits for our companies and for Europe as well.

The second reason is that there's a separate agreement called the umbrella agreement, which is a law enforcement agreement, where the Judicial Redress Act is actually an intrinsic part of that agreement and has to be finalized before the agreement is itself going into effect.

If I might, Mr. Chairman, if I could ask unanimous consent, there's an op-ed that I published in today's Hill on this very issue, if I could ask unanimous consent that it be included in the record of the Committee hearing.

Mr. CONYERS. As soon as I see it.

Mr. MACCARTHY. Okay.

Mr. CONYERS. Ms. Espinel, how does the recent invalidation of the U.S.-European Safe Harbor agreement impact the software industry?

Ms. ESPINEL. Thank you. So we are very concerned about the revocation of the Safe Harbor, and it has implications not just for software, but across our economic sectors. The cross-border data is used by nearly 5,000 companies, some of them large, many of them quite small, that use it to do all sorts of things, including process payrolls so that their employees get paid at home.

So we have significant concerns about the European Court of Justice decision that undermine the process put in place by the Safe Harbor. That said, we do think there is a path forward, and we think there are three things that need to happen: The first is that we need as, quickly as possible, to have the U.S. and the European negotiators come to agreement on a new Safe Harbor; the second thing is we need to have some reasonable, appropriate period of time for companies to be able to come into compliance with the

new rules under that Safe Harbor; but third, because we know this will continue to evolve and change, we need to work together, the United States and Europe, industry and Congress, on coming up with a global, sustainable long-term solution. It's clear that we need a new global framework for data and how it moves. And that needs to be an important part of the process as well.

I'll just say lastly, going to the point that Mr. MacCarthy made, passage of the Judicial Redress Act by the House is tremendously helpful, and so we thank all of you for your vote on that, and we hope the Senate follows your lead. That is, you know, important, both for our own domestic system, but is also helpful in terms of concluding negotiations on the Safe Harbor with Europe.

Mr. CONYERS. Thank you.

Thanks, Chairman Issa. I yield back.

Mr. ISSA. Thank you.

We now go to the gentleman from Ohio, Mr. Chabot.

Mr. CHABOT. I thank the Chairman for yielding, and also for holding this very, I think, important and very interesting hearing this afternoon.

It has been mentioned that barriers to free trade in the digital arena have a particularly adverse impact on small businesses, and I happen to be the Chairman of the House Small Business Committee, so I'd just like to ask—give each of the witnesses an opportunity to address what steps should be taken, specifically, to address this adverse impact on small businesses.

And I'll start with you, Mr. Allgeier, Ambassador Allgeier. If that's okay, and I'll just go down the line. If you don't have anything to say, that's okay, too, but——

Mr. ALLGEIER. No. Thank you very much.

What we find, of course, is that the digital technology has opened the world to small businesses. I mean, in the past, let's say a small business wanted to go overseas, well you'd have to find an agent, and you'd have to have a presence overseas. Now you put your product up on the Internet, whether it's a good or a service, and it's called random exporting. You don't know whether your next customer is coming from Boise, Idaho, or Bangladesh.

And then with the combination of express delivery and electronic payments, you're in the international market. And so it's extremely important that the movement of data remain open, and that people be able to have access to the Internet, and particularly small businesses or people in poor areas.

Mr. CHABOT. Thank you.

Dr. Atkinson.

Mr. ATKINSON. With the way the European Commission is negotiating the Safe Harbor, it's possible and hopeful that that will happen. But if it doesn't, people are talking about other possible ways that companies can get access to finding corporate rules and other types of model agreements. Those are clumsy, they're expensive, they're time-consuming, but large corporations can do that. Small companies really can't, and that would be the real harm here, or the biggest harm.

And so that's why I think we have to really insist that we put these very strict rules in trade agreements so that companies don't have to do these very expensive workarounds with—particularly in

Europe where they'd have to go to 28, or if you include the German lander or the states there, perhaps almost 40 different jurisdictions to be able to move data. And if you're a small company that's doing business in all of those jurisdictions in Europe, it's going to be almost impossible for you to be able to do that.

Mr. CHABOT. Thank you.

Ms. Espinel.

Ms. ESPINEL. So I think the risks and some of the options for small companies can be even more serious than for the large companies. So I would say a couple of things: One is specifically with respect to the Safe Harbor, as I said, the United States and Europe need to come together on a new agreement as quickly as possible. There needs to be some appropriate period of time for companies to come into compliance.

And then we need a long-term sustainable solution. But picking up on what Dr. Atkinson said, part of that is making sure that we have a good global framework for how data moves around and pushing back on restrictions of data.

You know, when I think about kind of the moment that we're in with data, and, you know, we live in a world where data is increasingly important, not just to big companies, but to small companies, not just to software, but to all of our sectors, it is an interesting fact that there is no comprehensive enforceable trade rules on data.

So it's kind of—you know, we're sort of at the moment that intellectual property was back in the Uruguay round, when the WTO was being established. There were no global rules on intellectual property in the trading system. That was a very difficult negotiation, but it was also very farsighted, on behalf of the United States and the other trading partners, to come together at the end of the Uruguay round, and agree to a global framework for intellectual property rules.

And I think that is exactly the moment that we are in right now with data. It is clear that it is a complicated new issue. It is also clear that it is going to be a driver of the U.S. economy and the global economy, and we need U.S. and other countries to lead on this issue and establish a global framework.

I think TPP, we understand, it could be—based on what we know about it, it could be the beginning of that. I think it's a real historic opportunity. But we are going to need to have those rules applied broadly across the world.

Mr. CHABOT. Thank you.

Mr. Black and Mr. MacCarthy, I've only got about 30 seconds left.

Mr. BLACK. My colleagues have been very articulate. Let me just stress that we are in a new era, and digital trade, if we want to make a metaphor back to original trade, blocking a Web site, doing various kinds of barriers or like blocking a port, and the openness of the trading system and going forward is so much tied to data and digital activity.

And Ms. Espinel is absolutely right. We need—our laws are based on historical outdated concepts of what trade is about. And we really need to see—and that's why we call for some precedent-setting efforts in the WTO to bring some cases to start relaying

some criteria and ground rules for how the problem should be dealt with.

Mr. CHABOT. Thank you. Mr. Chairman, is it okay if Mr. MacCarthy answers real quickly?

Mr. ISSA. Without objection.

Mr. CHABOT. Thank you.

Mr. MACCARTHY. The one point I'd add to everything else my colleagues have mentioned is that in this global framework for data, which I think is a great idea, we have to make sure that whatever rules affect the flow of data, whether they are privacy rules or consumer protection rules, or whatever, they're narrowly crafted, that they're least restrictive of trade. We can't take away the option for countries to enforce their privacy of consumer protection laws, but they can't unnecessarily trample on cross-border trade.

Mr. CHABOT. Thank you.

I yield back, Mr. Chairman.

Mr. ISSA. I thank the gentleman.

We now go to my colleague, the gentlelady from California, Ms. Chu.

Ms. CHU. Thank you, Mr. Chair.

Dr. Atkinson, you state that several countries around the world are limiting free trade in data, and you argue they are motivated by privacy and security concerns, national security and law enforcement concerns, and the desire for economic growth. The European Court of Justice recognized that the U.S. lacks an adequate level of protection for EU data amongst other privacy concerns.

Within this context, can you tell me how the EU views individual privacy and data security, and to what laws or principles do they have in place and what do we have in place here in the U.S.?

Mr. ATKINSON. Thank you. The Europeans culturally look at privacy differently than Americans do. As a general rule, they look at privacy as a fundamental human right. We look at it as a consumer right that has to be balanced against a number of other issues.

There's a lot of good scholarly evidence that shows that the European privacy directive and the rules that they have there actually significantly limit the Internet economy in Europe. There's a reason why the Europeans don't have global leaders in the Internet space, by and large. The effectiveness of their companies is significantly limited because of their privacy rules, and there's a very good study by Catherine Tucker at MIT who has demonstrated that.

Having said that, there's also another broad generalization that, I think, has some merit to it, which is, that we have less stringent rules, but we do a better job through the FTC and the State AGs of enforcing them than the Europeans do. They have stronger paper rules, but less real enforcement.

Having said that, I'll just close by saying, I don't think that we're miles apart. We generally share the goal of privacy. We share the goal of the rule of law, and I do think that we can work this out in a cooperative manner as long as the Europeans are willing to be reasonable, as we need to be reasonable.

Ms. CHU. So what, then, do you think should be done by Congress or by the Administration in these ongoing negotiations with

the EU to ensure that we're providing adequate privacy protections for our citizens, and for those whose data travels to our country from across the Atlantic?

Mr. ATKINSON. So I think there's two key points there: One is, I believe that we shouldn't sign a trade—a TTIP agreement with the Europeans unless it includes strict and enforceable rules around the free trade-in of data. I don't see why we should have that trade agreement if we don't have that component in there.

At the same time, there are steps that we need to take with regard to government access of data in the U.S. that have made the Europeans rightly uncomfortable, and I do think we need to do a better job there. And the Judicial Redress Act was one step in that, but I think there are other steps we can and should take.

Ms. CHU. Can you describe which countries have the most stringent regulations when it comes to setting limitations on data flowing in and out of their country? And what effect does that have an American companies' ability to compete?

Mr. ATKINSON. Sure. So we listed a number of countries in the written testimony, and what's troubling about that is if you look at that list, say in 2010, it would be significantly smaller: Nigeria, Turkey, Greece, Malaysia, Australia, Indonesia, Russia, China. China, just within the last year, for example, has put in place a set of—a numerous set of policies that would—that will significantly limit the ability for American companies to process data there.

So it really is something that's growing. There's a couple of Canadian provinces that do this as well. And I think one of the challenges really is their—they falsely believe that by doing this, that they will enhance security and privacy, commercial privacy. And I just simply reject that notion. I don't believe that's the case.

Ms. CHU. Ms. Espinel, you argue that as a result of that invalidation of the EU-U.S. Safe Harbor, many routine commercial dealings between the U.S. and European countries have now been disrupted. Can you give us an example of this?

Ms. ESPINEL. An example of the impact that it's having?

Ms. CHU. The disruptions that are occurring today?

Ms. ESPINEL. So, you know, an example of an impact that could happen if data stops moving back and forth is the ability to process payroll, as an example. Warranty information that U.S. consumers rely on would be at risk. So there are a number of real-life development—real-life impacts.

In cybersecurity, one of the maxims is that information is to follow the sun. So if you have information about a threat, you want to have that in the hands of cybersecurity experts, wherever they are in the world while they are awake, and restricting the data moving back and forth in the United States and Europe could put that at risk.

So I think there are a number of real world impacts. But, you know, even at a more macro level, the promise and the efficiencies that are brought about by cloud computing and by data analytics simply do not work if information cannot move around as efficiently as possible.

And I think one of the things that the trade barriers in the various countries that we see around the world, and the situation in

Europe is putting at risk, is putting a shadow on an industry that has enormous potential, but is still at a relatively early stage. And I think putting a shadow on the development of where remote computing can go and where data analytics can go at this early stage of its development is extremely troubling.

Ms. CHU. Thank you. I yield back.

Mr. ISSA. I thank the gentlelady.

We now go to the Vice-Chairman of the Subcommittee, the gentleman from Georgia, Mr. Collins.

Mr. COLLINS. Thank you, Mr. Chairman. I appreciate it.

Ms. Espinel, I want to go back to something, and then I've got others, too. Back in October last year, 2014, many of my colleagues, including myself, wrote a letter to the U.S. trade representative about the TPP. And just to review, first—we had several things: First, we wanted to include provisions that specifically keep borders open to free flow of data; second, it must prohibit countries from acquiring the use of local data servers and computing infrastructure as a condition for providing digital service; third, it must ensure nondiscriminatory treatment of digital products and services.

Based just on the reports that have come out so far from the Administration and others, where do you think we are in that right now?

Ms. ESPINEL. So, again, with the caveat that we have not seen the final text, our understanding is that the TPP has strong commitments on all of those provisions. First, on cross-border data trade and on pushing back on data localization; obviously, we would like that to be as comprehensive as possible. But our understanding is that, overall, the commitments there are strong. Our understanding is that there are prohibitions on imposing Custom duties on digital services, which is also important.

And our understanding is that, I believe for the first time ever, there are prohibitions on forcing companies to disclose source code in order to compete in a market. Those are all very important to us. And, again, based on the reports that we have heard, TPP contains strong and enforceable rules in those areas.

Mr. COLLINS. And granted, I think we will see those, and that's part of our whole process. But if that was not there, and probably a short answer is, if these protections were not there, given the new marketplace of the future that we're looking at, that being much more in this round, than it is for rounds and others, would that be a serious hindrance to enactment of this agreement?

Ms. ESPINEL. Well, I hope and expect that they are there. If they were not there, I think it would be an enormous missed opportunity. We were talking earlier about the fact that this is really the future, not just of the U.S. economy, but of the global economy as a whole. There are also enormous societal benefits that come from data analytics in cloud computing.

Mr. COLLINS. I agree.

Ms. ESPINEL. And in order for us to see the potential of those, it's enormously important that we have a global system of trading rules that gives clarity and predictability to the system.

Mr. COLLINS. Thanks.

Mr. Atkinson, real quickly, could you please describe for the Committee the problem of forced localization, and how this impacts member companies and your ability to create American jobs? Mr. Atkinson.

Mr. ATKINSON. So one of the real advantages the U.S. has is in cloud computing, for example, where we have north—it's in my testimony—north of 70 or 80 percent of—maybe even more—of the global market, partly because we have scale in our own domestic market that's given our companies the ability to scale up and get capabilities.

Other countries look at the cloud computing industry as a core strategic industry for their countries. And one of the ways that they're trying to gain market share is by simply saying that you have to store data out, not just in country, but, in some cases, in country with a domestic company. And that——

Mr. COLLINS. It could present a load of problems on many different levels?

Mr. ATKINSON. Pardon me?

Mr. COLLINS. It could present a load of problems on many different levels?

Mr. ATKINSON. Yeah. Even if it is just simply localization to tell an American cloud provider you have to put a server in a country, that essentially raises cost. If it was cost effective, they would have already done it, by definition.

Mr. COLLINS. Right. Okay.

Mr. ATKINSON. Not only does it raise cost, but something people haven't talked about, it has environmental impacts. Cloud computing, by putting it all in one place, you can save a lot of energy by requiring servers all over the world. So either way, whether it's forced server localization or domestic company preferences, it's going to hurt U.S. companies and the U.S. economy.

Mr. COLLINS. Mr. Atkinson, I appreciate that.

Mr. Black, very forceful in this Committee discussing some issues, but I've noticed something. We do read through all of your printed text before you appear. And on page 8 of your written testimony, you seem to want to have it both ways, and I think it's a concern.

The first way is you basically say that U.S. Internet intermediary liability and copyright rules discourage investment in growth and domestic startups. Yet, two sentences later in the same paragraph, you say U.S. businesses have thrived domestically under carefully crafted legal framework of U.S. law.

Now, you're basically contradicting yourself there. I don't know why you would do that, but I think one of the things that goes back for me is, is something I have said in this Committee from the day I came on, strong copyright, strong protective laws are not a barrier, but they're a creative incentive. I believe that what we—the framework that we have here has allowed U.S. Internet businesses to thrive, and they become a growth for your association and for many others that grow this industry.

So my question is, why are we presenting what seems to be a false narrative here, on one hand, saying that it discourages, and on the other hand, two sentences later, saying it encourages?

Mr. BLACK. Thank you very much for the question. Barriers to international trade data flows are a problem that we all talked about how important the economy of the future is.

Mr. COLLINS. Whoa, whoa, whoa. Your word says "domestic."

Mr. BLACK. We look at what made our society, what in the U.S. law has worked to help build our industry. Part of it is the balanced copyright. We have a very important, well-developed, well-refined system that provides both strong copyright protection and significant limitations and exceptions. That is a key to the health and vitality of what has allowed the Internet to flourish here.

And we believe it is, likewise, and it is appropriate, for the U.S. Government as we try to persuade others in the world to have strong copyrights, that they also reflect the boundaries and limitations that have proved so important to the ability of Internet and Internet companies to flourish.

Mr. COLLINS. It's an interesting question because -it's an interesting answer, because it frankly doesn't answer my question. Why would you contradict yourself? I understand that you want to say that—but when you said domestically U.S., it's either hindering or it's helping. You can't have it both ways in the same four sentences.

Mr. BLACK. Maybe I'm not——

Mr. COLLINS. You cannot say the U.S. Internet liability and copyright rules discourage investment and growth in domestic startups, and then two sentences later say, "U.S. Internet businesses have thrived domestically under carefully-crafted legal framework in the U.S." Either the legal framework we have here is bad, or the legal framework we have here is good. I believe it to be good. I'm not sure why it would be contradictory there.

Mr. ISSA. Would the gentleman yield?

Mr. COLLINS. Yes.

Mr. ISSA. If I heard that, Mr. Black, were you saying that the international conundrums are causing problems, while the domestic well-crafted has allowed us to thrive. Is that what your intent was in that paragraph?

Mr. BLACK. Yes, that's correct.

Mr. COLLINS. Well, the problem is—and that would be fine if understood, except that the footnote is to a footnote to a domestic—you know, saying which gives you the realization that it was for that. And this isn't something that our—you know, we've had many meetings on this from different various interests.

So I think the biggest thing is—the safe way to put this is, I believe that as we look at this, this is crafted in a well way. We continue to craft our copyright laws. It's going to help us all in this bigger picture, and not settling for what is a weaker system in other parts of the world, and I think we can——

Mr. BLACK. I would just suggest, weaker is the wrong terminology. A strong system is a balanced one. Just the same way as a three-legged stool versus a two-legged stool. The fact that you have balance and limitations in your system makes it stronger, not weaker.

Mr. COLLINS. Mr. Chairman, I yield back.

Mr. ISSA. I thank the gentleman.

And without objection, Mr. Black, if you want to revise and extend that portion to clarify it, I'm sure the Committee would be happy to have that record be full and complete.

And with that, we go to the gentlelady from Washington State, Ms. DelBene.

Ms. DELBENE. Thank you, Mr. Chair. And thanks for calling this important and timely hearing.

And thanks to all of you for being here with us today.

First, I want to start with Ms. Espinel. As you state in your testimony, quote, "In striking down the Safe Harbor, the Court of Justice focused on issues around national security and law enforcement access to data. Troubled by the Snowden leaks, the court concluded that countries that permit indiscriminate surveillance and interception, and mass and undifferentiated accessing of personal data could not be deemed adequate under EU law," end quote.

While the national security piece is certainly something familiar to members of this Committee, could you elaborate a bit on why the EU might be concerned about current U.S. law on law enforcement access to data?

Ms. ESPINEL. Yes. And I think it's, in part, because the rules in that area, as in other areas, are unclear. So, you know, one of the things that I think is clear is that we need a new global framework. And part of that needs to be addressing the fact that the rules right now on how U.S. law enforcement and foreign law enforcement can access data in the trading partners are unclear.

You are one of the cosponsors and introducers of the LEADS Act. We think that that would be—that approach would be a helpful part of the solution. We think it would be helpful, both, because it would give our businesses, but also their customers, whose data they keep, and law enforcement, a clear and predictable framework for how to access information.

We additionally think it would be helpful because without that, we fear our current system in the United States will open the door for foreign governments to be able to reach back into the United States for the data of our citizens, and that is a situation is that we would like to avoid.

Ms. DELBENE. And are there examples right now that you've seen in terms of how the lack of certainty has impacted businesses today?

Ms. ESPINEL. Yes. So there are a number of examples. There's a case that is actually being litigated right now in the U.S. courts between Microsoft and the Department of Justice involving data that is held in an Irish data center. The Department of Justice, making a request to get that data, and Microsoft's view that the request is inappropriate under U.S. law.

That is a real-life example that is being litigated in the courts right now. We will see what the outcome from the courts are, but we are concerned that if the outcome of that case is inconsistent with the position that Microsoft has taken in which the software industry is supportive of, as a whole, that this will open the door to other governments being able to reach back into the United States.

And so there is a domestic issue that we need to resolve absolutely, but part of the reason that we are so concerned about that

is because of the international implications of that and what that would mean for our system and the privacy of our citizens back at home.

Ms. DELBENE. Thank you.

You know, I had a meeting with a group visiting from the EU a few weeks ago, and someone—part of that group from the EU said that he felt like Americans don't care about privacy. And so are we contributing to that negative narrative about how privacy is viewed in the U.S. by failing to address some of these questions and policy ourselves?

Ms. ESPINEL. I think there are differences in approaches between the United States and Europe. But I reject the notion actually that United States and Europe are that different on privacy. Yes, Europeans care deeply about privacy. Americans care deeply about privacy, too. It is enshrined in our Constitution. We have a long history of protecting privacy.

I think there are improvements to our laws that have been made, or are in the process of being made. So I think the USA Freedom Act was a significant step forward, and I thank all of you for that. I think Judicial Redress Act is also a step forward, and hopefully, again, the Senate will pass it.

I think one of the things that will be really helpful in the environment that we live in today is for there to be a constructive dialogue between the United States and Europe to truly understand our different systems. Because as I said, I don't think the differences are as far apart as people sometimes portray them.

And if I could respectfully make a request of the members of this Subcommittee, I think when you're in discussions with your European counterparts, I think one of the things that would be very helpful is to explain to European counterparts how our privacy system works in the United States, some of the recent improvements that have been made in the privacy system, and try to lessen the amount of misunderstanding that I think exists today.

Ms. DELBENE. Thank you.

I wanted to get one more quick question in for Dr. Atkinson. You spoke earlier about things that you thought we could do to bolster our credibility and standing to fight data protection, and you talked about kind of some of the other steps we could do beyond judicial redress, which we just did. And I wonder if you could be more specific and tell us about some of those other steps we could take with our own privacy laws.

Mr. ATKINSON. Sure. I would second what Ms. Espinel just said, and go to the case in the court right now with the Microsoft Ireland case. And I think it's a very important case, because if the principle in the U.S. is that we can access data on a foreign person without going through that country's law, just because it's hosted by an American company, there will only be one result and that will be American companies will not host foreign person data in other countries. That will be the result.

The Europeans, the Irish, they will just simply say, you cannot put your data on an American cloud provider, regardless of where it's located. That can't be the result we want, and that's why the LEADS Act is important. That's why as part of the LEADS Act, one of the components in that is strengthening the MLAT process.

If the Justice Department wants access to that data, they should go through the MLAT process. The MLAT process could and should be better and faster and more streamlined, but that really has to be the direction we go, otherwise it just means that countries will just say you can't put data with an American company anymore.

Ms. DELBENE. Thank you.

Thank you, Mr. Chair. I yield back.

Mr. ISSA. Thank you.

We now go to the gentleman from Pennsylvania, Mr. Marino.

Mr. MARINO. Thank you, Mr. Chairman.

I know my colleague and coauthor, Ms. DelBene, asked direct and pointed questions concerning the LEADS Act, so I don't want to get into rehashing that. But is there anyone on the panel that wants to respond even further because of—given the fact that Ms. DelBene ran out of time? Please.

Mr. MACCARTHY. Thank you for that. The LEADS Act is an important piece of legislation. If the court case that——

Mr. ISSA. I'm afraid you're going to have to use Mr. Black's microphone.

Mr. MACCARTHY. Is that better?

Mr. ISSA. Yeah.

Mr. MARINO. Much.

Mr. MACCARTHY. So the LEADS Act is a very important piece of legislation. And if the court case that Microsoft is involved in goes the wrong way, there would, indeed, be disastrous consequences for U.S. companies.

But I wonder if a small amendment to the LEADS Act to make sure that it doesn't inadvertently encourage data localization wouldn't be in order. To the extent that it says to companies store the information in this country, and it's safe from the U.S., that, I think, would encourage people to store data in one location rather than the other.

Instead, the real stand, or issue, would be the nexus between the government and the data subject. If they're citizens or residents, then local laws should apply; if they're not, then local law should not necessarily apply.

Mr. MARINO. Okay. I'll ask that our staffs review your statement and others to see how we can make this more effective.

Anyone else? Ms. Espinel.

Ms. ESPINEL. I would just say briefly that I think these are clearly new issues, and they are complicated issues. I think the introduction of the LEADS Act and the work that's done—and I thank both you and Ms. DelBene for your work on that—demonstrates that while they are new issues and they are complicated issues, we as the United States, can still show leadership on these issues and try to move forward with various ways to approach them.

And I think that's extremely important. I do think that we need to bring other governments into that. I think having international consensus around these issues is going to be very important. But the United States, I think, will inevitably need to show the way. And I thank members for their leadership that has already been shown on this issue.

Mr. BLACK. If I could just jump in briefly. I think we are all on agreement an MLAT and LEADS. To understand the complexity

and why we have to be careful, whether it's EU or us, trying to come up with the solution, the answer of is data owned or located, a conversation among the five of us, if we were sitting in different countries and it was a video capture of that, it would, in fact, be stored around the globe on different servers, be in the cloud. So do each of us own it? To what rights do the others have to stop it, block it, disseminate it? We get into very complex issues.

We believe we can find answers, but quick, easy, simple answers in this area is very difficult. Ownership of data is a very tricky concept, and trying to precisely identify—the Microsoft case is very interesting because they've identified that the data has a location. A lot of people view the data they have on their servers disseminated through multiple servers, partly for security purposes.

So the answers—the questions here are very tricky. The answers need collaborative between governments, multiple governments and private sector players to come up with solutions, which is why we're nervous about imposed solutions, kind of rigidly applied in a regionally-limited area.

Mr. MARINO. I'm not sure if my colleague went into this area. If she did, perhaps you could expand on it; if not, take a shot at it. Give me your impression or what you've heard or what you see or think about the LEADS Act potentially having an adverse effect on U.S. law enforcement, compared to the abilities that they have now to obtain information from other countries? Dr. Atkinson.

Mr. ATKINSON. Well, I think it's a question of do they look at their access in a short-term or long-term perspective. In the short run, at the margin, it makes it slightly harder for them to get access to that data. In the long run, it will make it impossible to get it, or much more difficult to get access to that data.

Because as I said before, the dynamic will be, if the rule is that the U.S. can compel a U.S. company to turn over data with the lower standard on a foreign person that's stored in their country, countries will just mandate that that data cannot be stored with the U.S. company, and that will make it harder, not easier, for a law enforcement to get that data.

Mr. MARINO. Ms. Espinel, you have 9 seconds.

Ms. ESPINEL. Sorry?

Mr. MARINO. You have 9 seconds.

Ms. ESPINEL. I would just say, the Department of Justice right now is in a situation where they don't know exactly what the rule is. And that lack of clarity, predictability is not helpful for law enforcement either. I think the LEADS Act would be helpful in making it clear and predictable for everyone involved, including law enforcement.

Mr. MARINO. Thank you. I yield back.

Mr. ISSA. Thank you.

Gentleman from New York is next, I think, or from Rhode Island. Which one of you is ready to go first? The gentleman will yield to the gentleman from New York.

Mr. JEFFRIES. Thank you, Mr. Chair.

And I want to thank the witnesses for their presence here today and for very thought-provoking testimony.

Let me start with Ms. Espinel. There have been some concerns that have been raised by some of the people that I represent, and,

indeed, many aspects of the American public about sort of the downside of development of big data, the privacy concerns with respect to this data being misappropriated, abused, and misused.

But I was wondering if you could speak to some of the potential upsides, the transformative nature of big data as it develops to improve, you know, the quality of life, or address social conditions or improve the functioning of the economy as we move forward.

Ms. ESPINEL. I would be happy to. I will start by saying that our company take the privacy issues very seriously, so those do need to be addressed.

But, you know, I think we are living in exciting times. So here is a kind of incredible fact: If you look at all the data that exists in the world today, 98 percent of it was created in the last 2 years alone. That is extraordinary. That is obviously without precedent, and that is a rate of change that is going to continue to increase.

That has enormous implications for businesses, but it also has enormous implications for human beings who can use that data. And already today, even though this is an early stage, I think, for data, we're seeing enormous societal impact. So we're seeing them, you know, in cities that are using them to reduce pollution. Doctors are using data to make diagnoses more quickly.

There's an example that relates to saving lives of premature babies that are in NICUs that is, sort of, personally very meaningful to me. There is research being done on Alzheimer's. Farmers are using them to increase their yields while reducing the use of pesticides. So I think the societal benefits from data, data used properly, are enormous.

And beyond that, there are enormous economic benefits. So a conservative estimate of the gains from efficiency—so one of the things that businesses in the United States and Europe and around the world say is that using data helps them to be more efficient. And generally speaking, they report sort of a 5- to 6 percent increase in efficiency.

If you take a very conservative estimate and assume that there will be a 1 percent gain in efficiency, we are talking about creating $15 trillion to the world economy by 2030. That is equivalent to another U.S. economy. So both from the economic point of view, from the ability of small businesses, as panelists talked about before, to have access to international markets in a way that was never possible before, and in terms of some of the societal benefits we've seen, there is enormous promise.

And I will just conclude by saying, while there is enormous promise, it is early days. And so one of the reasons that we are concerned about some of the trade barriers that we see around the world is because we fear it will cast a shadow on innovation to come.

Mr. JEFFRIES. Now, the international concerns that many on the panel have spoken to in the context of trade, and some of the court decisions that we've seen come out of Europe, I want to turn inward for a moment and ask you, Ms. Espinel, do you think that the United States, in the face of this exponential growth of data in such a short period of time, as it relates to that 98 percent figure, do we have an adequate legal and regulatory framework in place right now, or are there things that this Committee, that this Con-

gress should be thinking about in this new data era that we exist in?

Ms. ESPINEL. I think it's inevitably the case that legal systems around the world are going to need to adjust to the world that we live in. You know, there's country's individual laws, and then there's sort of the global trading system that also needs to address.

And we've talked about some of the pieces of legislation that we think could be helpful, like the Judicial Redress Act, in trying to repair—be part of the solution to getting us to a new Safe Harbor. We've talked about the LEADS Act. You know, I think this is a rapidly-evolving landscape, so I think it's entirely possible that we will need further legislative change in the United States, and I am very confident that we will need legislative change in other countries of the world.

And I will close by saying, I think it is imperative that we have a global trading system that sets up strong and enforceable rules or data. Without that predictability around the world, I think it will be very difficult, not just for U.S. companies, but for all companies.

Mr. JEFFRIES. And in the limited time that I have, you mentioned the importance of American leadership, but you also said that it was important to develop international consensus. Could you speak to what some of the international challenges may be as it relates to how other international actors look at big data, which perhaps may differ than our view here in the United States?

Ms. ESPINEL. So I could talk about this almost indefinitely. I will try to be very brief. So I'll just highlight a couple of things: One is, I think, you know, other countries, sometimes the motivations are about trying to grow their domestic industry or trying to keep U.S. industry out of their markets. And so that is a reason, or can be a motivation for why countries put in place restrictions to keep barriers out.

But I think, you know, as I alluded to before, I think part of the issue is that these are new cutting-edge issues. And so I think not just the United States, but countries around the world are struggling with how do you balance security and privacy appropriately?

And so that is why I think, while I believe the U.S. will and needs to show leadership on this, I also think it's incredibly important that it's not the U.S. going out and saying this is our solution, and we think this should be imposed on the rest of the world. I think there does need to be international consensus.

I am fully aware of the fact that not every country in the world is going to want to be, or be able to be at that table right away, but I do think there are a number of countries where the United States could start having discussions about what norms of those areas should look like, and that would be very productive.

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

Mr. ISSA. We now go to the gentleman from Texas, who has been patiently at the end of the dais.

Mr. POE. Thank you, Mr. Chairman.

Thank you all for being here.

I want to talk about a specific issue of privacy: Surveillance by government. That's what I'm talking about. Not cybersecurity or any of those issues. Let's focus on that one issue.

To me, the United States has always been the world leader in privacy. We have a Fourth Amendment that you're all familiar with. Many countries, maybe most don't have such a concept as the Fourth Amendment, protection against unreasonable searches and seizures by government.

Mr. Atkinson, you talked about the Europeans use privacy as an excuse for really protectionism. I want to delve in this a little further and, talk about and ask you your opinion. There are three issues that we have regarding government surveillance on Americans. And if the perception of the Europeans is that America doesn't protect the right of privacy, perception, whether it's reality or not, is part of the reason we have this issue with the Europeans.

And one of those is the concept of the FISA courts; the second is surveillance under 702 warrants; the third is backdoor searches, and encryption that government may encourage our businesses to have into their systems; and the fourth is EPCA, whether it should be reformed or hasn't been reformed.

Those four issues to me, and I'm a former judge, are issues where it seems that government intrusion in those four areas and the failure for us, Congress, to redefine or define the Fourth Amendment to make sure it applies in those four areas or not may be part of the problem we have with dealing with foreign countries on the issues that you've all talked about.

So my question is—and I want all five of you to weigh in on this, I just want your opinion—does Congress, in your opinion, need to look at each of those four issues, those four areas where government surveillance on citizens is allowed, and fix that problem, or look at those four issues? What do you think about that issue as regarding government surveillance on citizens and the effect it has on businesses being able to have the free flow of data around the world?

So that's really the only question I have, and I'd like to just start and go down the row and see what you all think about that.

Mr. ATKINSON. I would agree with that. I'm less familiar, not an expert on the FISA court issue, but on all the other issues you brought up, I fully agree with you that we do need FISA reform on 702.

EPCA, we've been a long supporter of it. It really is illogical that there is a lower standard of government access to data that's stored in the cloud than data that's stored on my home computer. It just doesn't reflect technological reality that we would treat those differently. If we—so I fully agree with you on that.

And I do think all of that, and including the backdoor issue and the intentional weakening of U.S. systems, that all of those things have hurt our ability to be a global technology leader, and they're going to continue to hurt us until we take steps on it.

I will just say, though, and I think we need to be a little bit more vocal about saying that is, there are other countries that are doing things like that. If I were the Irish data protection authority, I wouldn't let Irish data go to France. In other words, there are other countries that do these as well, and I think it's important that we make that, that we're not the only country that has challenges there.

Mr. POE. I know other countries don't observe the concept of the Fourth Amendment, but we do in this country.

Mr. ATKINSON. Exactly.

Mr. POE. And I just want to know if that is a factor in this entire discussion.

Any others? We've got just about a minute left or less than that to weigh in on that.

Ms. ESPINEL. Just briefly. Yes, I think those are all areas that Congress should consider. I would speak to two of them. We are concerned about movements undermining encryption and we've made that clear. And we also very much support EPCA and would urge its quick passage by Congress. Thank you.

Mr. POE. Anybody else?

Well, I'm going to yield back my 9 seconds.

Mr. ISSA. And I'm going to take the 3 seconds back and treasure them always.

Oh, I'm sorry. I think—the gentleman is recognized for a short addition to his now expired time.

Mr. BLACK. Thank you. Very good points. Frankly, the world looks at what we do, not just what we say. If we're going to be a moral leader for an open, free Internet, we need to walk the walk as well as talk the talk. And those are all areas where we need to do more.

Without a doubt, I should point out there was a story that appeared today about the United Kingdom that just basically—apparently it was either finally passed, or very close to passing, a requirement that companies turn over—or have encryption that can be broken. That would be a terrible precedent, and the U.K. does it. Other countries are doing——

Mr. ISSA. Ms. Espinel, are you familiar with that?

Mr. BLACK. We're the only ones that do some things. Governments want to have access to information that's global.

Ms. ESPINEL. Yes. I should just say—and I will check on this—but we have been concerned about the U.K.'s moves toward requiring backdoors to encryption and have raised that with the U.K. Government. My understanding is that most recently, the U.K. Government has stepped back from that and has said that they are not going to be requiring backdoors to encryption in the legislation that is moving through the U.K. system.

So I will check to confirm that and come back to you. But we view that as a very positive step, because, not to take too much time, but part of the reason that we are concerned about encryption here in the United States is not just because of here in the United States, but because of the precedent overseas.

And so if my understanding is correct, and the U.K. Government yesterday said they would move forward with their legislation without those requirements to backdoors, we view that as, at least, one positive step in this discussion.

Mr. ISSA. Mr. MacCarthy, if the gentleman would—okay. Please.

Mr. MACCARTHY. Very briefly. I agree with——

Mr. ISSA. Again, you've got to use Mr. Black's microphone. We've denied you full access, I'm afraid.

Mr. MACCARTHY. Equal access to microphones.

Mr. Poe, I agree that those are issues that need to be addressed. I agree that back doors are a problem. We would oppose further movements in that area for the reasons that have been articulated. We're strong supporters of EPCA. But my point is that none of those things need to be preconditions for a successful resolution of the negotiation for a new workable Safe Harbor.

Mr. POE. Thank you, Mr. Chair.

Mr. ISSA. And with that, I'll take those 3 seconds and pass them on to the gentleman from Rhode Island for an additional 3 seconds.

Mr. CICILLINE. Thank you, Mr. Chairman.

Thank you to the witnesses for this very useful testimony, as we sort of struggle with this question of how do we preserve cross-border data flows, and if we're really making the point of how important this is to our economy, and how unsustainable a system that interrupts those flows would be in the long term.

And you've all spoken about the need for a narrowly-crafted, but least-restrictive-of-trade kind of standard. And I want to sort of press you a little bit on that, and beginning with you, Mr. Ambassador. You make the same argument, of course, in your written testimony that we need a workable, and commercially-viable and legally-valid alternative to the Safe Harbor provision.

I wonder if you could just expand on this a little bit, and describe what you think should be included in such an alternative. And also, how do your member companies plan to take privacy concerns into account until such a new standard is developed?

Mr. ALLGEIER. Well, thank you very much.

Yes, it is very important for all of our companies, because they're all dealing with cross-border data flows, that there be a successor to the now invalidated Safe Harbor. And I think it goes a lot back to what Rob Atkinson was saying, is that there's going to have to be a workable way of recognizing some of the differences in privacy laws, but also make it viable for companies to actually comply with it without making it completely chaotic.

I'm not a lawyer, so I don't have specific suggestions on how do we work that, but I think that—as Victoria said, that once there is a successor, there needs to be sufficient time for companies to come into compliance.

So I think there should be a recognition that, all right, if we've reached agreement, we leave the existing system in place for a reasonable period of time. And then these 4,000 companies—and some of them are small companies, a lot of them are—need time to then show that they can meet the new requirements of Safe Harbor 2.0, or whatever it's called.

Mr. CICILLINE. Does anyone else have a suggestion? Yes. Dr. Atkinson.

Mr. ATKINSON. I would agree with that, although I think ultimately, we're going to have to move beyond the Safe Harbor to a formal trade agreement. I know people have alluded, for example, to the WTO protections—or exemptions around—in the services agreement around moving from privacy and security. Unfortunately, what we're seeing are countries that are using that as a guise for protectionism, China being a case in point.

I have talked to Chinese Government officials who tell me that they're justified in doing what they're doing because of national se-

curity concerns, which is just simply false. Under the way the WTO rules are set up, it's hard to bring that case. And I don't see any evidence that we're going to change the WTO rules anytime soon.

That's why it's important to put this in trade and services agreement, and a TTIP agreement with a very, very, very narrow exception so that countries can't use that to drive the truck of mercantilers through——

Mr. CICILLINE. May I just follow up, Dr. Atkinson. One thing you said in your written testimony is that the European Court of Justice overturned the Safe Harbor agreement, not because of privacy concerns, but because of concerns about governmental access. Does it then sort of follow that either as part of the Safe Harbor, the new agreement, or in conjunction with it that we put into place additional surveillance reforms to respond to that concern raised by the court? Sort of building on Judge——

Mr. ATKINSON. I would argue that it does follow from that. I would say two quick things, though: One is, they made that decision without any real judicial review. They must have just watched some videos from—you know, that was shown, you know, what NSA did or something. There was no real collection of evidence when they made that decision, and I think that should be very troubling.

Secondly, as I said earlier, they haven't cut off other countries who have more problematic access, government access rules than we do. But having said that, I do think it's incumbent upon us to make some reforms that would go in that direction, as you said.

Mr. CICILLINE. And just one final question for the panel. Does Congress have a role to play, and if so, what is it, in establishing this sort of modernized Safe Harbor framework? Is there a useful role that Congress can play in the development of that?

Ms. ESPINEL. Sure. So I would say, there's a short term and a long term. I think short term, we need to encourage the United States and Europe to come to an agreement on new Safe Harbor. We don't believe—we do not believe we need new U.S. legislation to do that, although we do hope the Judicial Redress Act passes as soon as possible. And I think Congress has a role to play in working with your European counterparts to encourage Europe to come to the table and to reach an agreement as quickly as possible on a Safe Harbor 2.0.

But then looking at the long term, I think it is also clear that is not our long-term solution. We're going to need a global solution. We're going to need something that is flexible and principled-base, and I think Congress absolutely should play a role in working with the Administration and working with industries and working with your counterparts around the world and helping to determine what that long-term solution is going to look like.

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

Mr. ISSA. Thank you.

We now go to the gentlelady from San Jose.

Ms. LOFGREN. Well, thank you. This has been very interesting, and I appreciate the insight shared by all the witnesses to the Committee.

You know, I think that we are in for a very tough time, actually long term, in trying to reconcile very different approaches to free-

dom, essentially. If you take a look at what the European Court of Justice did, they basically said that the 2000 Commission had erred by failing to take into account the interaction of U.S. domestic law and U.S. international policy and the framework; in other words, it didn't take in the whole picture, and it's going to allow the data protection agencies in each country to investigate violations. Well, where does that lead us?

I mean, you've got a situation in Europe, and I—as Ms. DelBene mentioned, many of us meet with the parliamentarians from Europe, who feel that their decision on right to be forgotten is extremely important to them and very valuable. And when you get into it with them, you say—I mean, recently, an agency in France ruled that links in content removed under their right to be forgotten has to be removed worldwide. And when you talk to them about, Hey, we have a First Amendment. Even if we agreed with you, we can't agree with you. I mean, we can't allow elimination of First Amendment rights.

So when you talk about data, I think it's—it depends on which kind of data you're talking about. I mean, if you have a database that is the product of the health study, and it's completely owned by, you know, a university, it's possible to control the sharing of that data in a very different way than a posting on Facebook. You know, I think we're looking—we're looking down the road at some very severe—and I'm not sure how we get to a situation that's going to be suitable. But getting to that, I'm wondering—you know, Mr. Black, you mentioned the right to be forgotten and others have talked about it, is a major barrier to data flow. How do you see this ending up when you've got the First Amendment that protects Americans' right to free speech, and a Europe that has no equivalent respect for speech, but has an equivalent right to—to sensor? How are we going to resolve this?

Mr. BLACK. Well, as I tried to indicate, it's a very troubling concept. And when you think about it, if it becomes an established precedent, and we are seeing other countries in other parts of the world are considering similar versions, it is an amazing shield for basically hiding data, distorting history, limiting the ability to prevent, frankly, honest information transfer. We talked about "data," and we all use "data," and it's important we do, but we're talking about information and knowledge, and the ability to block information and knowledge, to block people's ability to communicate part of communication is getting information. It's a very serious precedent.

And unless it is whittled down, and we find some way to back off of its broad reach—I mentioned the editorial aspect that's exceptionally troubling, but frankly, even if you don't go to that step, the breadth of the concept of the right to be forgotten, the ability—and we all want database to be cleaned up of erroneous fact, but, again, it is, once again, imposing a liability on players, intermediaries, that is fundamentally a flaw, and you can do it on—for so many purposes. You can——

Ms. LOFGREN. Right.

Mr. BLACK. And we had this discussion earlier, but if you have intermediaries liable for what users do, or for what information or

data that flows over the networks, you will have a crippling of the open Internet as we know it today.

Ms. LOFGREN. Well, what I see, I mean, going—I'm sorry Mr. Marino had to leave, but we have Safe Harbors in the DMCA, and we have section 230 of the Communications Decency Act. We have some provisions that is would allow the Internet to flourish. They don't have that in Europe. And so I think that's part of the reason why they don't have an Internet economy. They have crippled their tech sector in that way and maybe a few others.

And to think that you can control the flow of data and have an Internet, that's not how the Internet works. So I—I think that we have a fundamental misunderstanding with some of our colleagues in parliaments across the world. That's not to say there aren't countries that are just using this as an excuse. I mean, you take a look at countries that want to have localized data; Russia, China, Turkey, these are not companies that—countries that are, you know, wallowing in free speech. They have a different agenda.

I just want to make one final comment on—or maybe even a question, on copyright. Because, you know, we've also got a problem there, and it's a crossover with free speech. We recently had a situation where European book publishers are saying that you can't actually index their books, and that if you index their books, there would be an index tax. Which is—I remember when people wanted to do an email tax. That's not going to happen. And so I've been telling the parliamentarians, if they look ahead in Europe, they're going to be like China, because we're going to have to cut them off, because we're not going to lose our freedom because they don't value theirs.

Do you see it going in that direction?

Mr. BLACK. This is an excellent area for action to actually be taken by the U.S. Government. Under the Berne Convention, okay, it is very clear there is a right in order to basically have access to news. We think if the U.S. Government wishes to, some of these snippet tax approaches are, in fact, challengeable under existing law. We all want—we've all said we want to improve the rules governing data flow around the world, but there are some rules that are in effect now that are not being utilized. And in this area, we think there's room for action immediately to go after some of these more egregious attempts to, frankly, alter the rules of access to information.

Ms. LOFGREN. Mr. Chairman, could I just have 1 second more to make a comment?

When Spain said you can't link to news articles, and Google just withdrew, and then none of the newspapers could find readers. So I think to some extent, there's a role for the government to play, but I think, also, companies are going to have to take actions themselves, because they can't live with some of these rules. And I think when the European public can't actually access information, there's going to be reaction among the public themselves.

Thank you, Mr. Chairman. I yield back.

Mr. ISSA. Thank you. And I thank you for that salient point. I think it is one of those where be careful what you wish for. May Spain always have the dark ages back, if that's what it wishes for.

Dr. Atkinson, I'm going to ask you sort of a question that I know the answer to, but—but it may be a will question as much as it can.

Would be it helpful and/or appropriate and/or possible to sue the EU under the WTO in light of their decision?

Mr. ATKINSON. So, I'm not a trade lawyer, and I know when Ira Magaziner made those veiled threats back in the late '90's to get the Europeans to come to the table on Safe Harbor, he did suggest that we file a suit with the WTO. I think the case is stronger now, as I said earlier, because they haven't just said they're cutting—they've only cut us off. They haven't cut off other countries who have even less governmental protection. So I think there is possibility. And I think we shouldn't back down from holding up the—as Teddy Roosevelt in—speak softly but carry the big WTO stick.

Mr. ISSA. I'm sure WTO was in that.

Let me ask a broader question. I had the opportunity to be in Antarctica last year. Fifty-three Nations—I had to look that up to remember—53 Nations are all part of an international treaty that says you can go there; you can have things there; you can't—you can't mine and take the resources, and nothing could be done there that essentially isn't agreed to by the party as a whole. It's a non-country by international agreement.

As this Committee goes forward with the number of pieces of legislation, and we're looking at privacy, domestically, and then we're looking at a global world, do—I'd like each of your comments briefly, just as we have around our Custom systems, if you will, sort of free trade zones, they have places where you can bring your goods to the United States, but they're not in the United States for any practical purpose. And there's no tariff, and quite frankly, they are still considered to be not in the country. So they can only be seized or looked at as a ship might be bordered in international waters.

Should we use, if you will, a combination of these two models, the pretrade zone in the U.S. and the idea just like Antarctica, there have been to be places, in this case, the cloud, in which all countries have to view it as outside their reach, and as such, not so easily taken whether it's in the U.S., and Europeans are concerned that their privacy will be breached, or vice versa, inside another country where somehow the standard would be artificially higher or lower to enforce whatever is subject to what I would envision as an international trade agreement that mirrors, if you will, the best of the protections of, let's say, the Europeans and ourselves and other partners.

Can I have your comments on that?

Mr. ATKINSON. Sure. One of the reasons we're having this debate right now over privacy, it's emblematic of a broader set of questions a number of the panelist members have brought up. And, really, what we lack is we lack a consistent, readily understandable and shared global framework for thinking about governing the Internet. And by that, I don't mean ICANN governance. I mean, all of the policy questions that countries face with regard to the Internet. We don't have a shared view of what's appropriate, what's not appropriate. And I think we have to—we've proposed in that a recent re-

port called the "Framework For Resolving Cross-border Internet Policy Conflicts." And I think we—I think it's incumbent upon——

Mr. ISSA. And I appreciate that, and I'd love you to answer further, and I'll read any material you send me. My question was more narrow, is should we take away in some hosting environments, if you will, a cloud and say it does not reside inside the U.S., even though it's in Toledo, but, in fact, it doesn't reside in any Nation, and all Nations have to observe at the same level of respect as though one might do an extradition, rather than a simple subpoena, no greater, no less than—than that? And that's one of my questions is, if we're going to make the cloud a free trade zone, do we have to begin looking at it as not ours, even if it's in the U.S. and not theirs, even if it's hosted there. And I'll just go down the list. But please stay narrowly focused, because I want to get to Mr. Johnson.

Mr. ATKINSON. I disagree. I'm not sure that is exactly the right way to go, because there are legitimate things government has access to and concerns that are legal. And if it's in the cloud, it shouldn't be extraterritorial, in my view, should be covered by a trade agreement.

Mr. ISSA. Just so you know, the Chairman of the full Committee made it very clear in the last round of legislation that this Committee was tired of our country knowing more about us than us knowing less about them. So you may—you may find the definition of legitimate interest to the government is on the wane from this Committee rather than the ebb it had after 9/11.

Ambassador.

Mr. ALLGEIER. I thought your metaphor was very interesting, because the free trade zone, as you say, the products are in there and you can do all sorts of things with them. But once they leave that zone, they are subject to whatever the duties are and the regulations are of the markets they are going into. So I don't know if it's perfect, but in a sense, the cloud is where it resides, and then only when it leaves the cloud for a particular reason does it become subject to, well, whatever the jurisdiction is of whatever is being used. It's an interesting thought.

Ms. ESPINEL. So I would just say, I'll take that to be a serious proposal, and I would like to give it serious consideration. But I could just make two observations, free trade zones work, in part, because they fit inside of a global trading system that has rules. And so, I think part of—a prerequisite to this would be to have that global trading system of rules for data.

Mr. ISSA. By the way, I think it was about 1959 that we started trying to get Antarctica. We are only at 53 countries. So I have no illusions that this would necessarily be quick and easy, but it is—it begins to appear to me that if we do not begin to think of the cloud as not America's, then the rest of the world will say, if it's going to be yours when it's in America, then it's going to be mine if I have the ability to mandate it. And that's—that's exactly what this hearing today was about, is how do we get that free flow to be not a bias toward a country of residence to the detriment of others concerned?

Mr. Black.

Mr. BLACK. I think it's an intriguing idea. I agree it should get some serious considerations, look at the ramifications. I hate to use metaphors I haven't thought out ahead of time. But, you know, when we talk about the oceans, we have territorial waters, and then we have the open sea. And it may well be there's a certain appropriateness here to think of things that are not—should not be geographically, and therefore, governmentally tied to one Nation. I would like to explore that more.

Mr. ISSA. Mr. MacCarthy, as you answer it, I want to tell you—yeah, grab the right one—I did not use the high seas, because there's too much seizing of things on the high seas, but rather, places in which the world has agreed to a common set of protection, a common set of respect for other countries. Nobody can go into Antarctica and do something where other countries are not essentially consulted in the process. So it is a little more like extradition and a little less like the high seas.

Mr. MacCarthy.

Mr. MACCARTHY. So I think the idea is worth exploring in great detail. I'm worried that even our own regulators who have a responsibility to protect the privacy and the anti-fraud interests of our own consumers would want to gain access to information in order to enforce local law. And so the idea that there could be a place of the cloud, the Internet, that is literally a place without law, that probably is the right way to go.

But the next step of trying to harmonize the rules probably is difficult. We've heard the difficulties in the First Amendment. We've—privacy is also a very, very difficult issue to get harmonized laws. We have got a sectorial approach. The Europeans have a different approach. But you can make those rules interoperate. That's what the Safe Harbor was supposed to be all about, and that's why we have to get it back into place as soon as possible.

Mr. ISSA. Okay. I'm going to go to Mr. Johnson. But I will leave you with this, because we can certainly, many of you we regularly have a dialogue with. If the United States is to lead, we certainly have exclusively, within our jurisdiction, the ability to create these zones. We have the ability to lessen our own authority over a site hosted under this concept that it is not America without specific protections. In other words, a foreign hosting site, to use a term that may not exist yet.

But, you know, the United States could, tomorrow, decide that we're going to have foreign hosting sites, and that a foreign hosting site is, by definition, one of which the Department of Justice and others must treat it as a non-U.S. and use an open and transparent process in order to go after it, and not treat it quite the same as we would a U.S. In other words, give it all the protections of being in the U.S. from a standpoint of the NSA not being able to hack it, and yet, give it additional protections.

This is not a new concept to think about, can we do better? The question is, will America lead? And that's what I'd like to have in the days and months to come.

Your comments on can America lead by creating something which the rest of the world could have a higher belief on, and if we do this, the same as we created the Internet, and we set the standards and then we gave it as a gift to the world, at least as

to entities which are hosted within our borders, but are hosted under some enhanced protection and assurances for the rest of the world, we could lead a standard that I doubt that Russia and China would follow, but I certainly would like to reach a standard that the EU would admire and emulate.

Mr. Johnson, I apologize for going a little long, but the gentleman is recognized.

Mr. JOHNSON. Well, no. In fact, I'm—I'm prompted to yield whatever time that the gentleman would extend to me, the 5 minutes. I tend to think that I might be better off by just simply yielding to you and listening to your questions. There's a lot that I missed having been absent at an Armed Services Committee meeting, and I don't want to go over plowed ground. I'm just kind of here to learn. And so with that, I will yield back to the Chair.

Mr. ISSA. I thank the gentleman.

Is there anyone who wants to make any closing remarks that, from the whole host of questions that you would like to have briefly in the record, and then we can—you can extend, and I'll say in that my closing remarks.

Mr. MacCarthy.

Mr. MACCARTHY. So very briefly. It's very good news that the European Commission has suggested that there's an agreement in principle on the Safe Harbor. We have every reason to expect it will see a rapid conclusion of that. Commissioner Jourova is coming over here in a couple of weeks, maybe he will do something there.

They have every incentive to get this right. Digital trade between the United States and Europe is huge. We have a global trade surplus of $150 billion in digital trade. They have a global surplus of 163. They know that their fundamental interests are at stake here, and I think they are going to try to act to try to put in place a Safe Harbor to make transatlantic data flows work again.

Mr. ISSA. Mr. Black.

Mr. BLACK. Very short.

Mr. ISSA. Reclaiming your mike.

Mr. BLACK. Very short. A lot of consensus I think you heard today. The reality is that we're going to have a lot of these problems linger for a while. There are no easy solutions. The Internet is a tremendous part of our future. I would—I guess I would urge, as a U.S. citizen, that we had a huge role in creating the Internet. We have a tremendous history and essential one to the First Amendment, freedom of speech, as we go forth and set rules domestically or internationally, that we keep it to a forefront of our principles, that commitment to openness, the freedom to access information, and that has, frankly, created a climate that has allowed the Internet to flourish.

If we do that, we're gonna still have a lot of problems to wade through, but keeping our eyes on that fundamental set of principles will lead the way. Thank you.

Mr. ISSA. Ms. Espinel.

Ms. ESPINEL. Thank you. Well, I would start off by thanking you for holding this hearing and focusing on attention on this issue. Having been given the extra time, I would just reiterate two things I said before.

Mr. ISSA. You can just tell us, what was it like being at E&C versus here? Which Committee did you think better of? You can be impartial here.

Ms. ESPINEL. Clearly, this one.

Mr. ISSA. Of course.

Ms. ESPINEL. I think in terms of the trade barriers that we have talked about, we have been playing policy Whac-a-Mole for over 5 years. There are countries around the world that have been considering trade barriers, putting trade barriers forward, and our hope and expectation is that TPP will be, at least, a start of a mechanism to push back on those. And so if it does what we believe that it does, it is a truly historic opportunity.

The second thing is just, if I could go back to the U.S. EU's Safe Harbor, because it is sort of an issue of immediate concern. I agree with Mr. MacCarthy. All indications are that that we will—the United States and Europe will be able to come to a quick conclusion on the Safe Harbor 2.0, but anything that Congress can do to encourage U.S. and Europe to come together on that would be—would be great, but we need to bear in mind that if the Safe Harbor is concluded, and if there's an appropriate period of time for U.S. companies to come into compliance, that—that will only get us so far, and then we are going to immediately need to turn to working out what our long-term solution will be. Because I do not believe that the next Safe Harbor will be that long-term solution.

Mr. ISSA. Anyone else? Doctor.

Mr. ATKINSON. I think one of the things that's been happening in the last few years is that the policy realities have finally caught up to the nature of the global Internet and not in a good way. And I think the challenge that we face, both here and around the globe, is we have to figure out a way to balance the differences that we have between countries, legitimate differences in values and cultures. We're not all going to agree. We can never do that. And so we have to figure out a way to allow the Internet to thrive and flourish in a system where people are going to have different rules and different policies.

At the same time, we have to be able to have a way that global free trade and data goes on, and goes on in a robust way. And I think we can square that circle, but it's really gonna require not just all the specific actions that we've talked about, which are important; it's going to require a larger conversation along the lines of what you've proposed. A much bigger way to think about this and the way to bring in countries, like the Antarctica problems that we tried to solve. We need something like that at the global level now.

Mr. ISSA. Ambassador, you get to close.

Mr. ALLGEIER. Thank you very much. Well, these issues that we've been talking about, cross-border data flows, localization, open Internet, and so forth, should be subject to rules that are multi-lateral, and the place normally to do that would be the World Trade Organization.

The World Trade Organization is not operating at this point in a way that we can do that. And so our second best alternative is to get these issues right in each of the negotiations that we're undertaking, whether it's the TPP, the one with Europe, the one on

services, bilateral investment treaties with China. At least try to get a cohesive and right approach in all of those to create *de facto* the template. The advantage of the WTO, if we can get it there, is that there is dispute settlement. It's legally binding, and so, for example, if there's a dispute about whether somebody is using a—a health reason or a prudential reason for protectionism, you can at least battle it out within a legal framework there.

So I think that's what we should ultimately be looking for, but in the meantime, we need to get it right in the other negotiations.

Mr. ISSA. Well, I want to thank you all of you for a delightful conversation back and forth. I think to all of us who attended, this was very useful.

As promised, I will leave 5 legislative days to submit additional written materials on any subject, but particularly the ones that I brought up. And if you have any additional extraneous material, we also would accept that.

And with that, we stand adjourned.

[Whereupon, at 3:54p.m., the Subcommittee was adjourned.]

APPENDIX

Material Submitted for the Hearing Record

Prepared Statement of Edward M. Dean, Deputy Assistant Secretary for Services, International Trade Administration, U.S. Department of Commerce

Testimony of
Edward M. Dean, Deputy Assistant Secretary for Services,
International Trade Administration, U.S. Department of Commerce
Before the House Judiciary Subcommittee on Courts, Intellectual Property, and the Internet
International Data Flows: Promoting Digital Trade in the 21st Century
November 3, 2015

I. Introduction

Good Morning, Chairman Issa, Ranking Member Nadler, and distinguished Committee Members. Thank you for the opportunity to submit written testimony about the U.S.-EU Safe Harbor Framework. I have welcomed the high-level attention Committee Members have brought to Safe Harbor since the October 6 European Court of Justice (ECJ) decision. Your statements, letters and outreach have highlighted the importance of Safe Harbor to U.S.-EU trade and the need to promptly endorse the strengthened Framework that we have negotiated with the European Commission during the past two years. With over 4,400 companies in the United States utilizing the program, it is a cornerstone of the transatlantic digital economy enabling growth and innovation in the United States and in Europe. As a result, it is my top priority and is a top priority of our Secretary of Commerce and the Administration as a whole.

In my capacity as Deputy Assistant Secretary for Services in the International Trade Administration, I oversee the team administering the Safe Harbor Framework at the Department of Commerce and have led our consultations with the European Commission over the past two years to update Safe Harbor. In this testimony, I will provide a brief history of the Safe Harbor Framework and our engagement with the European Commission. I will then discuss the ECJ decision, its implications and our work to ensure data flows between the United States and EU can continue.

II. History of the U.S.-EU Safe Harbor Framework

The Safe Harbor Framework has, for 15 years, served as a model for the protection of privacy while facilitating data flows that fueled growth and innovation on both sides of the Atlantic. Safe Harbor was developed by the U.S. Department of Commerce and European Commission following the adoption in 1995 of the EU Directive on Data Protection (EU Directive 95/46/EC). The EU Directive came into effect in 1998, restricting the transfer of personal data to non-EU countries that did not meet the EU "adequacy" standard for privacy protection. While the United States and the EU share the goal of protecting the privacy of our citizens, the U.S. approach to privacy, which includes sectoral privacy legislation, state laws, and robust enforcement by the U.S. Federal Trade Commission, has not been deemed adequate by the EU.

In order to bridge these differences in approach and provide a means for U.S.-based companies to receive data from the EU in compliance with the EU Directive, the U.S. Department of Commerce in consultation with the European Commission developed the Safe Harbor Framework. The Safe Harbor Framework was designed as a voluntary, enforceable code of conduct based on globally-recognized privacy principles to which U.S.-based companies could self-certify. Under Safe Harbor, U.S.-based companies voluntarily certify their commitments to

Safe Harbor's data protection requirements. In doing so, those companies' public commitments and attestations became enforceable by the U.S. Federal Trade Commission. The Safe Harbor Framework was deemed "adequate" by the European Commission and EU Member States in 2000. The Department of Commerce has worked closely with the European Commission since the program's inception to strengthen the operation of program within the parameters of the existing Framework.

By the time of the European Court of Justice ruling, over 4,400 companies in the United States were participating in Safe Harbor and relying on the European Commission's determination that it provided adequate protection to process data in the course of transatlantic business. These 4,400 participants come from nearly every sector of the economy. 61% of the companies are small and medium sized businesses with 250 or fewer employees. They include U.S.-headquartered companies, as well as U.S.-based subsidiaries of EU companies. While media focus has centered on data exchanged through social networks and as part of cloud services, Safe Harbor participants process a wide variety of data from Europe to conduct business. This includes human resources data of EU-based employees, shipping and billing information for the purchase of goods and services, and transactional data necessary to support 24/7 customer service. In short, the global trading and financial system today depends on the ability to seamlessly send and receive personal data without regard for national borders. This dependence is revealed by the more than $240 billion worth of digitally deliverable services trade between the United States and Europe. Safe Harbor ensured that this data could move both efficiently and in compliance with EU law.

III. Recent Developments and DoC Engagement

Following the surveillance disclosures in 2013, the European Parliament and some EU Member State officials called for suspension of the Safe Harbor Framework. The European Commission responded with a review of the Framework followed by the release of a Communication with 13 recommendations to improve the Framework. The first eleven related to commercial data flows and the last two pertained to national security issues. Following the release of the Commission's Communication in November 2013, the Department of Commerce initiated consultations with the Commission to address their recommendations.

Before describing the negotiations, it is worth saying a few words about the broader political context in Europe around these issues. Since Safe Harbor had become linked to the surveillance disclosures, it became a target for continued criticism largely based on misunderstanding and false assumptions about its purpose and operation and the important privacy benefits it provided. At their heart, many of these criticisms were based on false accusations that the United States was engaged in "mass, indiscriminate surveillance" of the data transferred to the United States under Safe Harbor.

For the past two years, the Department, along with the U.S. Federal Trade Commission and Department of State, has engaged in consultations with the European Commission. We have also worked with officials from the Intelligence Community and the Department of Justice to discuss the national security-related recommendations. Recognizing the importance of data flows and the challenging political context in which we were operating, we worked hard to strengthen the framework and address concerns raised in the EU. In our view, it was appropriate

to modernize the 15-year old Framework, and there were improvements and changes we could make that enhanced privacy protections while continuing to facilitate data flows. Throughout this process, we consulted regularly with U.S. stakeholders to discuss both the privacy benefits and commercial feasibility of potential changes. We were mindful of areas that might cause new compliance costs for U.S. firms and pushed back in our negotiation when we felt that any change might unduly burden U.S. firms relative to other companies. These were difficult negotiations, but over the summer we reached a tentative agreement that was subject to review and approval by the European Commission's political leadership. At that point, the Commission chose not to move forward given the pending issuance of the European Court of Justice Decision.

In its October 6 ruling, the European Court of Justice invalidated the European Commission's determination in 2000 that Safe Harbor provides adequate protection for personal data. This determination by the Commission was the legal foundation for Safe Harbor. The ECJ decision did not examine or make findings regarding the adequacy of U.S. protections; rather, it faulted the European Commission for examining Safe Harbor but not the broader U.S. legal context in 2000. Unfortunately, the ECJ decision did not allow a transition period for companies to make alternate legal arrangements, creating even greater legal uncertainty.

We are deeply disappointed in the ECJ decision, which creates significant uncertainty for both U.S. and EU companies and consumers, and puts at risk the thriving transatlantic digital economy. The ruling does not give adequate credit for the robust protections of privacy available in the U.S. or all that the Framework has done to protect privacy and enable economic growth. We are focused on and fully committed to resolving the uncertainty that the decision has created and thus end the significant, negative consequences that flow from such uncertainty.

We fully understand how harmful uncertainty can be to a business, its growth, employees, customers, and vendors, and have been hearing directly from companies, large and small, about the real world impact of the ECJ decision. We have stressed to the Commission that real harm is presently being borne by companies that have committed in good faith to protect privacy in accordance with globally recognized principles. It is worth emphasizing that the ECJ decision does not question whether U.S. companies provided their consumers with the protections promised under the Safe Harbor.

To illustrate just how harmful the uncertainty created by the ECJ decision has been, I offer two illustrative examples:

- A small company, which provides support services relevant to clinical research trials, has already lost significant business across Europe. The company's clients are suspending and shutting down projects, while its EU-based main competitor has reached out to other existing clients recommending they switch providers in light of the court ruling.

- A large U.S.-based hotel chain with properties across the EU would in the absence of Safe Harbor have to either: put in place EU model contracts with each of its vendors – something it described as a logistical nightmare – ; or, take on the EU's binding corporate rules process, which is very expensive and has an 18-month lead time.

While model contracts, binding corporate rules, and other options for compliance with European privacy law do exist, the ECJ ruling has also raised questions about their viability. For example, following the ECJ ruling, a German DPA released a position paper indicating that model contracts and consent might also be considered invalid for transferring data to the United States.

We believe the best way to protect privacy and restore confidence in transatlantic data flows is to promptly endorse and put in place the strengthened Safe Harbor Framework that we have negotiated with the European Commission during the last two years. We have provided a very strong basis for the European Commission to make the findings discussed in the ECJ decision, including on the national security issues. That being said, we are continuing to discuss ways to improve and strengthen the overall package now, and to be sure that it addresses the specific issues raised by the court.

This is a priority for me, for Secretary Pritzker and for the Administration as a whole. We have welcomed many of your own calls for this important step. Secretary Pritzker, senior officials at the White House and across the interagency community have been in close and regular contact with the European Commission, as well as other partners across Europe, including within individual Member States, and have expressed the need for urgent resolution of this issue. I was in Europe during each of the past three weeks meeting with the European Commission, EU data protection authorities, EU Member State officials and affected U.S. and EU businesses to discuss the path forward. Our Secretary, Deputy Secretary, and the Under Secretary for International Trade among other senior officials have also traveled to Europe during this time. Each has engaged on this issue both during their trip as well as from Washington.

IV. Conclusion

We remain committed to doing everything we can, as fast as possible, to move forward with a new Safe Harbor Framework. We are prepared to focus full time on this issue in order to bring greater certainty around the critical issue of data flows. We are hopeful that our partners in the Commission will be willing to approach this with the same sense of urgency, and we appreciate the focus you and your colleagues here in Congress can bring to this important issue.

Prepared Statement of Nuala O'Connor, President and CEO, Center for Democracy & Technology; and Gregory T. Jojeim, Director, Freedom, Security & Technology Project, Center for Democracy & Technology

Statement for the Record of

Nuala O'Connor, President and CEO
Center for Democracy & Technology
and
Gregory T. Nojeim
Director, Freedom, Security & Technology Project
Center for Democracy & Technology

House Judiciary Committee
Subcommittee on Courts, Intellectual Property, and the Internet

Hearing on

International Data Flows: Promoting Digital Trade in the 21st Century
November 3, 2015

(Submitted November 13, 2015)

Chairman Issa, Vice-Chairman Collins, Ranking Member Nadler, and Members of the Subcommittee:

The Center for Democracy & Technology (CDT)[1] submits the following statement for the record summarizing the necessary reforms to U.S. surveillance and privacy laws that must be made in order to ensure the viability of any future Safe Harbor agreement between the U.S. and the E.U. In *Schrems v. Data Protection Commissioner*,[2] the Court of Justice of the European Union (CJEU) not only struck down the Safe Harbor agreement (an agreement vital to transatlantic trade on which over 4,000 U.S. companies had relied for fifteen years); it also found that national Data Protection Commissioners (DPCs) in the E.U. are obligated to investigate complaints that a country that receives E.U. users' data – such as the U.S. – does not provide adequate protection for data privacy rights.

As a result, the *Schrems* decision will have lasting and, without reforms to U.S. law, recurring consequences for international data flows and digital trade. CDT acknowledges the value of approving a short-term "Safe Harbor 2.0" agreement in order to provide temporary relief. In addition, the Judicial Redress Act and Presidential Policy Directive 28 (PPD-28), which provide limited privacy protections for Europeans located abroad,

---

[1] The Center for Democracy & Technology is a nonprofit public interest organization dedicated to keeping the Internet open, innovative and free. Among our priorities is preserving the balance between security and freedom.

[2] Case C-362/14, *Maximillian Schrems v. Data Protection Comm'r* (Oct. 6, 2015), *available at*: http://curia.europa.eu/juris/document/document.jsf?text=&docid=169195&doclang=en.

are small steps in the right direction. However, legislative action that directly addresses the concerns that were at the heart of the CJEU's judgment is required in order to establish a stable, long-term agreement that will not be subject to persistent challenges by European DPCs and courts.

This statement first examines the background of the *Schrems* judgment and the European privacy laws underlying it. The statement then outlines the privacy rights that the Court indicated must be guaranteed with respect to Europeans' data in order for the E.U. to allow companies to transfer such data to the U.S, and provides an overview of some of the reforms that must be made to U.S. law in order to adhere to those privacy rights. We focus on necessary surveillance reforms because concerns about surveillance are at the heart of the *Schrems* judgment, and because they are within the jurisdiction of the Judiciary Committee. We conclude by emphasizing that although the *Schrems* judgment necessitates changes in U.S. law surveillance law, surveillance reforms must ultimately be global in nature in order to provide effective data security and protections for human rights. In addition, the U.S. data protection regime must be strengthened by passage of an effective Consumer Bill of Rights.

I. Overview of the *Schrems* Case

A. Origins

In 1995, before the widespread use of the World Wide Web and email, the European Union had the prescience to create the Data Protection Directive,[3] which mandates that personal data may only be transferred from the E.U. to a non-EU country if the latter "ensures an adequate level of protection" of privacy and other individual rights. In 2000, the European Commission, the E.U.'s executive body, decided that the U.S. offered an "adequate level of protection" and that it was therefore lawful for companies to transfer data from the E.U. to the U.S.[4] This decision was the legal basis for the Safe Harbor arrangement. Under that arrangement, U.S. companies self-certify that they will take certain steps to protect personal information, but such steps are subsidiary to company obligations to disclose personal information governmental entities for law enforcement or national security reasons.

Following the Snowden revelations that began in June 2013, Facebook user Maximillian Schrems filed a complaint with the national Data Protection Commissioner (DPC) in Ireland, alleging that the U.S. did not provide an adequate level of privacy protections, and asked the Commissioner to investigate whether Facebook should be allowed to transfer E.U. users' data to the U.S. The High Court of Ireland decided to refer to the CJEU the question of whether national DPCs in the E.U. had the authority to carry out

[3] Directive 95/46/EC of the European Parliament of the Council of Oct. 24, 1995 on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data, 1995 O.J. (L 281) 31, *available at*: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31995L0046:en:HTML.
[4] Decision 2000/520/EC (July 26, 2000), *available at*: http://eur-lex.europa.eu/legal-content/en/ALL/?uri=CELEX:32000D0520.

such an investigation, since the European Commission had already found in its 2000 decision that U.S. data protections were "adequate."[5]

B. The CJEU's Judgment

The CJEU concluded that not only are national DPCs able to investigate complaints that a non-E.U. country's protection of Europeans' data privacy is inadequate, but that the DPCs are, in fact, obligated to conduct such investigations upon receiving a complaint.[6] The Court also went a step further and examined the issue of whether the European Commission's 2000 decision underlying the Safe Harbor agreement was valid, and concluded that it was not.[7]

The Court recalled that in order for such an agreement to be valid, the non-E.U. country – in this case, the United States – must ensure "an adequate level" of data protection in line with E.U. fundamental rights laws. The Court then indicated that in order to be "adequate," protections in the U.S. (or any other non-E.U. country) must be "essentially equivalent"[8] to those guaranteed in the E.U. under the Data Protection Directive and the Charter of Fundamental Rights of the European Union[9] (effectively, the E.U.'s "Bill of Rights," which contains explicit rights to privacy and the protection of personal data). Critically, the Court went on to elaborate on the specific types of privacy rights countries such as the U.S. must guarantee in order to receive data from the E.U. These privacy rights point directly to reforms of Section 702 of the Foreign Intelligence Surveillance Act of 2008 (FISA) as well as the establishment of baseline consumer privacy protections.

II. Recommendations

A. Reforms to Section 702 of FISA

The data protection requirements described in the CJEU's decision are standards that U.S. law does not currently meet, thanks in large part to Section 702 of FISA. Although Section 702 is not scheduled to sunset until 2017, achieving an adequate level of reform will take time, and a failure to begin addressing the CJEU's concerns as soon as possible will result in any new Safe Harbor agreement being subject to constant scrutiny and instability. CDT has determined that the *Schrems* decision necessitates the following reforms to Section 702. These are reforms that the Committee should embrace not just because they would facilitate commercial trade, but because they would advance the constitutional rights of Americans in the U.S., the human rights of people on a global basis, and at the same time, begin to strengthen the tenuous constitutional foundation on which this surveillance now rests:

---

[5] Schrems v. Data Protection Comm'r, [2014] I.E.H.C. 310 (H. Ct.) (Ir.), *available at*: http://www.bailii.org/ie/cases/IEHC/2014/H310.html.
[6] Case C-362/14 at ¶ 63.
[7] *Id.* at ¶ 67.
[8] *Id.* at ¶ 73.
[9] Charter of Fundamental Rights of the European Union art. 7-8, 2000/C 364/01, *available at*: http://www.europarl.europa.eu/charter/pdf/text_en.pdf.

- **The prohibition of "upstream" surveillance**: The CJEU found that laws allowing government authorities to "have access on a generalised basis to the content of electronic communications" violate "the essence of the fundamental right to respect for private life."[10] When the U.S. government engages in "upstream" surveillance based on section 702, it temporarily seizes virtually all Internet-based communications flowing into or out of the United States.[11] Officials then search those communications for all those that are "to," "from," or "about" a given selector (such as an email address), gather that data, and store it for later searching (via queries) by the NSA, CIA, and FBI.[12] *Because "upstream" surveillance involves seizing and searching communications content so comprehensively and on such a large scale, without strong legal restrictions designed to ensure that both the seizure and searching are strictly necessary and proportionate, the Court is unlikely to uphold any future E.U.-U.S. data transfer arrangement unless section 702 is amended to prohibit this type of activity.*

- **A strict limitation on the purposes for which the U.S. may conduct surveillance under section 702**: The CJEU indicated that E.U.-U.S. data transfers should not take place unless the U.S. government can only gain access to (and use) the data "for purposes which are specific, strictly restricted and capable of justifying" the privacy intrusion involved.[13] The current wording of section 702 broadly authorizes the collection of telephone calls, emails, instant messages, social network content, and other communications content of non-U.S. persons reasonably believed to be located abroad so long as a "significant purpose" of that collection is to acquire "foreign intelligence information."[14] Therefore, so long as acquiring foreign intelligence information is a "significant" purpose, the U.S. government can intercept such communications for a plethora of other reasons. *The broad, opaque language of the current section 702 should be revised to prevent the executive branch from conducting surveillance under the program unless it is seeking to investigate or prevent a limited set of specific dangers, such as terrorism. Moreover, the bodies that have the power to search or otherwise gain access to the data that has been collected, as well as the circumstances under which they may do so and their transparency obligations, should be clearly set out in law.*

- **Stronger, more transparent authorization and oversight processes**: The *Schrems* Court stated that limitations to E.U. citizens' privacy rights must be

[10] Case C-362/14 at ¶ 95.
[11] Charlie Savage, *N.S.A. Said to Search Content of Messages to and from the U.S.*, N.Y. TIMES (Aug. 8, 2013), *available at*: http://www.nytimes.com/2013/08/08/us/broader-sifting-of-data-abroad-is-seen-by-nsa.html?_r=0.
[12] *See* Privacy and Civil Liberties Oversight Board (PCLOB), "Report on the Surveillance Programs Operated Pursuant to Section 702 of the Foreign Intelligence Surveillance Act," 7 (July 2, 2014) [hereinafter "PCLOB Report"].
[13] Case C-362/14 at ¶ 93.
[14] 50 U.S.C. § 1881a(g)(2)(A)(v).

"strictly necessary,"[15] and emphasized the need for strong safeguards against abuse.[16] Under current law, the FISA Court (FISC) does not approve any particular acquisition or target.[17] It does not even authorize the terms and phrases that will be used when querying the collected information. Instead, it approves proposed guidelines for targeting that are meant to ensure that the surveillance is focused on non-U.S. persons reasonably believed to be located outside the United States.[18] The FISC also approves proposed minimization procedures meant to limit the acquisition, retention, use, and dissemination of non-public information about U.S. persons acquired through Section 702.[19] *Congress should strengthen the authorization and oversight process for Section 702 surveillance by requiring FISC or other independent approval of the specific terms the intelligence agencies may use to search captured data. In addition, reforms should be adopted to make Section 702 authorization and oversight processes more individualized and capable of imposing firm, clear, and consistent restraints.*

- **A genuine ability for individuals whose communications might be subject to secret surveillance to obtain redress for any abuses**: In addition to highlighting the need to provide "minimum safeguards" that effectively protect data subjects from risks of abuse, the Court also emphasized the need for individuals to have some type of access to judicial review of decisions pertaining to their personal data.[20] The Judicial Redress Act was a limited first step[21] to affording non-U.S. persons a small degree of judicial review under the Privacy Act, but the Privacy Act provides no meaningful redress for targets of intelligence agency surveillance under Section 702 because the agencies can exempt themselves from the Act's requirements on grounds of national security (and have indeed done so).[22] *Congress should provide an effective judicial redress mechanism for individuals whose communications might be subject to Section 702 surveillance. This can be achieved by providing a right to standing for people who can produce evidence that they may have been unlawfully monitored.*

B. Reforming the U.S. Data Protection Regime

In addition to U.S. surveillance practices under Section 702, the CJEU's concerns in the *Schrems* judgment appear to have stemmed from an overall lack of confidence in the level of protection and respect given to consumer data in the U.S. The United States is one of only two developed nations without privacy protections for all personal data

---

[15] Case C-362/14 at ¶ 92.
[16] *Id.* at ¶ 91.
[17] *See* PCLOB Report, *supra* n. 12, at 27.
[18] *Id.*
[19] *Id.*
[20] Case C-362/14 at ¶ 95.
[21] For CDT's analysis of the Judicial Redress Act, see https://cdt.org/blog/the-eu-us-umbrella-agreement-and-the-judicial-redress-act-small-steps-forward-for-eu-citizens-privacy-rights/; 32 CFR § 322.7(a).
[22] 5 U.S.C. § 552a(k).

(Turkey is the other).[23] Instead, only a handful of sector-specific laws apply to narrow categories of information, coupled with the Federal Trade Commission's (FTC) power to combat some privacy violations as "unfair and deceptive practices" under section 5 of the FTC Act.

U.S. law must be updated to conform to the needs of the digital age. With the advent of increasingly sophisticated technologies that collect detailed personal information, there is a pervasive sense that consumers have lost control of their data. Worse, this exponential increase in personal data that is collected, shared, and stored for indeterminate periods of time is coupled with a rise in the frequency and scope of data breaches.[24] *The U.S. data protection regime should be brought up to date by passing a strengthened Consumer Privacy Bill of Rights*[25] *with substantive protections that track the Fair Information Practice Principles (FIPPs)-transparency, individual control, respect for context, focused collection and responsible use, security, access and accuracy, and accountability. Such protections should be predicated on individual rights and not conditioned on an assessment of privacy risk. In addition, they must be protected by robust enforcement mechanisms.*

III. Conclusion

We appreciate the opportunity to present our views to the Subcommittee about the need for reforming U.S. privacy and surveillance practices in order to enable the long-term free flow of international data. Although this statement for the record focused on reforms to U.S. law, CDT acknowledges that a truly effective solution to the problem of protecting personal information will have to be global in nature. Some who have examined the CJEU's decision in *Schrems* have rightly pointed out that many European countries' surveillance programs would not live up to the privacy standards mandated by the CJEU, and that they of late are moving backward, not forward, in terms of the protections they afford.[26] These troubling laws do not change the United States' need to reform its surveillance practices in order to facilitate the free flow of information for commercial reasons in light of the CJEU's *Schrems* decision, or its obligation to change Section 702 to protect human rights and civil liberties.

We look forward to collaborating with you on these important issues. For more information, please contact CDT's Greg Nojeim, Director, Protect on Freedom, Security & Technology, gnojeim@cdt.org; (202) 407-8815.

---

[23] *See* NYMITY, Inc., "Sectoral and Omnibus Privacy and Data Protection Laws" (2015), *available at*: https://www.nymity.com/~/media/Nymity/Files/Privacy%20Maps/NYMITY_World_Map.ashx.
[24] *See* Verizon 2015 Data Breach Investigations Report (April 13, 2015), *available at*: http://news.verizonenterprise.com/2015/04/2015-data-breach-report-info/.
[25] For CDT's analysis of the Obama Administration's draft Consumer Privacy Bill of Rights Act, see https://cdt.org/insight/analysis-of-the-consumer-privacy-bill-of-rights-act/.
[26] Press Release, Center for Democracy & Technology, Draft UK Surveillance Bill Would Do More Harm than Good to Privacy (Nov. 4, 2015), *available at*: https://cdt.org/press/draft-uk-surveillance-bill-would-do-more-to-harm-than-good-to-privacy/.

Letter from Michael Beckerman, President & CEO, The Internet Association

Internet Association

The Honorable Darrell Issa
Chairman, Subcommittee on Courts, Intellectual Property and the Internet
United States House of Representatives
2138 Rayburn House Office Building
Washington, DC 20515

The Honorable Jerrold Nadler
Ranking Member, Subcommittee on Courts, Intellectual Property and the Internet
United States House of Representatives
B-351 Rayburn House Office Building
Washington, DC 20515

Examining the EU Safe Harbor Decision and Impacts for Transatlantic Data Flows

Dear Chairman Issa and Ranking Member Nadler:

The Internet Association writes to express our views on recent events impacting the U.S./EU Safe Harbor. Cross-border data flows between the U.S. and Europe are the highest in the world and the free movement of data creates jobs and enhances growth on both sides of the Atlantic.[1] It is therefore imperative that data flows between the U.S. and the EU be supported in a way that provides legal certainty and continuity to businesses and consumers alike.

The Internet Association is the unified voice of the Internet economy, representing the interests of leading Internet companies[2] and their global community of users. The Internet Association is dedicated to advancing public policy solutions to strengthen and protect Internet freedom, foster innovation and economic growth, and empower users. Important to our mission is the advancement of public policies that support the free flow of data globally while promoting and protecting privacy. Until recently, the U.S./EU Safe Harbor framework served both these policy goals effectively. Over 4,400 US companies relied on Safe Harbor to validate the transfer of data from the EU to the U.S., including both U.S. headquartered companies and U.S. based subsidiaries of EU headquartered companies. Over half of these companies are small and medium sized enterprises.

---

[1] Joshua Meltzer, *The Importance of the Internet and Transatlantic Data Flows for U.S. and EU Trade and Investment*, Global Economy and Development at Brookings Research Paper (Oct., 2014), http://www.brookings.edu/research/papers/2014/10/internet-transatlantic-data-flows-meltzer.

[2] The Internet Association's members include Airbnb, Amazon, auction.com, Coinbase, Dropbox, eBay, Etsy, Expedia, Facebook, FanDuel, Gilt, Google, Groupon, Handy, Intuit, LinkedIn, Lyft, Monster Worldwide, Netflix, Pandora, PayPal, Practice Fusion, Rackspace, reddit, Salesforce.com, Sidecar, Snapchat, SurveyMonkey, TripAdvisor, Twitter, Yahoo, Yelp, Uber, Zenefits, and Zynga.

[illegible] 12th Street NW, Washington, DC 20005
[illegible] 12th Floor, West
www.internetassociation.org

Like the thousands of U.S. and EU companies who complied with the Safe Harbor in good faith, our members were disappointed when the European Court of Justice recently invalidated the Safe Harbor effective immediately. While the Internet Association respects that ECJ opinion in the Schrems case as binding and final in nature, we think it important to flag two issues with the court's analysis of U.S. law since they should be factored into the ongoing negotiations between the EU and the U.S. around the renewed Safe Harbor framework. These two issues are the court's analysis of U.S. surveillance law as well as its treatment of U.S. commercial privacy law in the Schrems opinion.

First, the ECJ Schrems opinion is premised on inaccurate assumptions about U.S. surveillance law that do not capture the significant surveillance reforms undertaken since 2013. The Internet Association and its members have consistently supported these reform measures, which should inform negotiations to revitalize Safe Harbor.

In the aftermath of the Snowden revelations, President Obama's Review Group on Intelligence Communications and Technology drafted a comprehensive report with a set of 46 recommendations concerning reforms to U.S. surveillance programs, laws, and intelligence agencies. Some of these recommendations formed the basis for subsequent legislation while others continue to inform the debate about broader surveillance reform measures. Separately, the Privacy and Civil Liberties and Oversight Board (PCLOB) published comprehensive reports with concomitant recommendations related to key sections of the Foreign Intelligence Surveillance Act (FISA) and the PCLOB is currently undertaking a review of Executive Order 12333.

In June this year, President Obama signed the USA Freedom Act into law. The USA Freedom Act prohibits the bulk collection of telephony and Internet metadata under various U.S. legal authorities, allows companies to publish transparency reports with further granularity around the volume and scope of national security demands issued by governmental entities, and codifies new oversight and accountability mechanisms.

The USA Freedom Act was preceded by Presidential Policy Directive PPD-28. PPD-28 provides that signals intelligence collected about non-U.S. persons may no longer be disseminated solely on the basis that the information pertains to a non-U.S. person. To the extent that signals intelligence is collected about non-U.S. persons in bulk, it must be for one of six specified purposes[3] and no others.

More recently, on October 20, 2015, the House of Representatives passed the Judicial Redress Act (H.R. 1428) by a voice vote. This legislation, if enacted by the Senate, would ultimately enable non-US persons to enjoy judicial redress rights given to U.S. citizens under the Privacy Act of 1974.

Unfortunately, none of these significant changes to U.S, surveillance law and oversight were analyzed by the ECJ in its recent Safe Harbor opinion. Significantly, these undertakings by the U.S. government

[3] Counter-espionage, counterterrorism, counter-proliferation, cybersecurity, detecting and countering threats against U.S. armed forces or allied personnel, and to combat transnational criminal threats.

[illegible] Washington, DC 20[illegible]
12th Floor, West
www.internetassociation.org

Internet Association

stand in stark contrast to the ECJ's view that the U.S. engages in "indiscriminate surveillance and interception carried out [] on a large scale."

Separate and apart from surveillance reforms, the ECJ Safe Harbor opinion did not acknowledge today's layered and effective U.S. commercial privacy enforcement regime. Since the late 1990s, the Federal Trade Commission has enforced its broad authority under Section 5 of its enabling statute over 100 times against data privacy and security violations that constitute "unfair or deceptive acts or practices in or affecting commerce."[4] Beyond this broad FTC jurisdiction, Congress has enacted several sector specific statutes protecting children's, financial, and healthcare information. And beyond Congress, the states have enacted over 300 privacy laws controlling a diverse array of issues - from data breach to employer access to their employees' social media accounts.

The U.S. Department of Commerce and European Commission have spent nearly two years renegotiating a renewed Safe Harbor agreement to address the Commission's concerns regarding the protection of EU citizens' privacy since the national security revelations of 2013. The revised framework will strengthen protections for EU citizens' data while facilitating transatlantic data flows that bring significant benefits to the U.S. economy and the EU economy alike.

It is important to the Internet Association that the ongoing Safe Harbor negotiations between the U.S. and the EU are premised on a fair and current understanding of U.S. law. In its Safe Harbor opinion, the ECJ laid out the standard for "adequacy" that would allow for continuing data flows between the EU and the U.S. and we are confident the U.S. regime, when fairly examined, would satisfy this standard. We therefore urge the Department of Commerce and the EU Commission to take into consideration the current state of *both* U.S. surveillance law and commercial privacy law in finding the common ground needed to reach agreement on a new Safe Harbor framework.

We urge the Department of Commerce to conclude the ongoing Safe Harbor negotiations as soon as possible and, in conjunction with the European Commission, announce the revised framework. The announcement of this framework will represent an important step in providing businesses with certainty and stability in their transfer of data across the Atlantic, and will reassure European citizens that their personal data will continue to be afforded the highest level of protection when it is transferred to the United States.

Respectfully submitted,

Michael Beckerman
President & CEO
The Internet Association

[4] 15 USC §45(a).

[illegible] 12th Floor, West
www.internetassociation.org

Letter from Daphne Keller, Director of Intermediary Liability, Center for Internet and Society, Stanford Law School

Stanford Law School

Center for Internet and Society

Crown Quadrangle
559 Nathan Abbott Way
Stanford, CA 94305-8610
Tel: 650 723-1417
daphnek@law.stanford.edu

November 2, 2015

The Honorable Bob Goodlatte
Chairman
House Judiciary Committee
2309 Rayburn House Office Building
Washington, D.C. 20515

The Honorable John Conyers, Jr.
Ranking Member
House Judiciary Committee
2426 Rayburn House Office Building
Washington, D.C. 20515

The Honorable Darrell Issa
Chairman
Subcommittee on Courts, Intellectual Property, and the Internet
2269 Rayburn House Office Building
Washington, D.C. 20515

The Honorable Jerrold Nadler
Ranking Member
Subcommittee on Courts, Intellectual Property, and the Internet
2109 Rayburn House Office Building
Washington, DC 20515

The Honorable Doug Collins
Vice Chairman
Subcommittee on Courts, Intellectual Property, and the Internet
1504 Longworth House Office Building
Washington, D.C. 20515

Dear Chairman Goodlatte, Ranking Member Conyers, Chairman Issa, Ranking Member Nadler and Vice Chairman Collins,

I am the Director for Intermediary Liability at Stanford Law School's Center for Internet and Society. I was previously Associate General Counsel at Google, where I handled both data protection and content notice-and-takedown issues for over ten years. I write to describe imminent changes to European Union law that will alter important parts of the landscape for international data flows. These changes are not part of the EU's technical "data transfer" rules, which will likely be discussed by witnesses at this Tuesday's hearing. They will nonetheless powerfully affect the movement of information across borders – as well as free expression, commerce and technical innovation on the Internet.

These changes are part of the nearly-final General Data Protection Regulation (GDPR), a far-reaching new EU law which has been under negotiation since 2012, and is expected to be finalized in December of this year. The GDPR stakes out unprecedented jurisdiction for EU regulators, including jurisdiction over many US companies. It requires those companies to retool their products and businesses, and appoint representatives in Europe to work with regulators. It also requires them to honor EU "Right to Be Forgotten" law, deleting or "de-indexing" online content that

is clearly legal in the United States. This deletion will likely be global, affecting the information available to Internet users everywhere including the United States. Key terms in the Regulation remain ambiguous and open to interpretation. But because local or national regulators will be able to assess fines of up to €100,000,000.00, those regulators' decisions will effectively govern US companies without deep coffers and an appetite for protracted legal battles in Europe.

The GDPR reflects values and priorities that are simply different from the ones we protect under US law. European legislators are choosing to impose regulatory burdens on innovation and commerce because of the high value they place on personal data protection rights – rights that in many cases have no equivalent under US law. Those rights are also often deemed strong enough to trump free speech rights, when the US First Amendment would mandate a different outcome. While this may be the right balance for the EU, it is not the one US law has ever struck. Applying the GDPR to US companies with US-facing businesses will effectively push those values across borders to affect innovation and free speech here.

Perhaps the most troubling aspect of the GDPR for US companies is its jurisdictional reach. The GDPR requires compliance from any company that "monitors" users in the EU – regardless of whether the company intended to attract EU customers, or even knew about them. Thus, it appears to give EU regulators jurisdiction over any American business that tracks user information using tools like accounts or cookies, and that has even a few European users. For example, the New York Times online would be regulated by the GDPR because of its user accounts and recommended articles feature. The same could be true for American content distributors, hobbyist websites, and small online goods vendors, and other businesses. Large Internet companies like Facebook, Twitter, and YouTube are covered as well. The GDPR's jurisdiction grab will be most surprising, and probably most damaging, for small and growing enterprises that achieve commercial viability at home only to discover they must undertake costly compliance with European laws.

Compliance with the GDPR is a heavy and expensive burden. Companies that may be operating out of garages in the US and fully compliant with US law will find themselves part of an intensively regulated industry in Europe – and likely already in violation of European law by the first time they hear about it. Penalties are steep: €100,000,000.00 or 5% of global annual turnover, in some drafts of the Regulation. To come into compliance, companies would start by stationing a designated representative in the EU; responding to any inquiries or requirements from regulators; curtailing collections and uses of data that are legal in the US but illegal in Europe; re-designing back-end data storage systems and front-end user interfaces; and petitioning European regulators for permission prior to launching particularly novel, "high risk" products or businesses.

To avoid violating the GDPR, companies must also comply with EU "Right to Be Forgotten" laws – by deleting content that is clearly protected under the US First Amendment. An existing version of the "Right to Be Forgotten" is already being enforced for Google's web search, and has eliminated[1] hundreds of thousands of

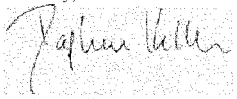
[1] https://www.google.com/transparencyreport/removals/europeprivacy/

search results in Europe. According to the Washington Post,[2] results that disappeared include news articles about a banker involved in the financial crisis and an article about a dishonest soccer referee. The Post also received[3] a demand that the paper remove a negative concert review from its own website – a demand the paper will have to take more seriously under the GDPR.

Extension of EU "Right to Be Forgotten" laws threatens US Internet users, as well as US companies. French privacy regulators already maintain that deletions required under their data protection law must be carried out globally – that French law should determine what information users in the US can find online. The only company currently affected, Google, has so far opposed this demand. But standing up for the rights of American Internet users to see information that is legal here requires a risk-tolerance (and legal budget) that smaller companies will not easily muster. The easiest and safest course for companies newly regulated by the GDPR will be to simply comply with deletion demands – to let EU law determine what information Americans see on the Internet.

I attach with this letter three short blog posts describing the GDPR's exact provisions and political background. They are also available online here[4], here[5] and here[6]. The regulation stands to be finalized in under two months, and has so far received little attention from lawmakers or media in the US. Given its foreseeable impact on American businesses and on free speech and innovation online, that should change.

Sincerely,



Daphne Keller
Director of Intermediary Liability

About the Center for Internet and Society
The Center for Internet and Society (CIS) is a public interest technology law and policy program at Stanford Law School and a part of Law, Science and Technology Program at Stanford Law School. CIS brings together scholars, academics, legislators, students, programmers, security researchers, and scientists to study the interaction of new technologies and the law and to examine how the synergy between the two can either promote or harm public goods like free speech, innovation, privacy, public commons, diversity, and scientific inquiry. CIS strives to improve both technology and law, encouraging decision makers to design both as a means to further democratic values. CIS

[2] https://www.washingtonpost.com/opinions/ungoogled-the-disastrous-results-of-the-right-to-be-forgotten-ruling/2014/07/12/91663268-07a8-11e4-bbf1-cc51275e7f8f_story.html

[3] https://www.washingtonpost.com/news/the-intersect/wp/2014/10/31/pianist-asks-the-washington-post-to-remove-a-concert-review-under-the-e-u-s-right-to-be-forgotten-ruling/

[4] http://cyberlaw.stanford.edu/blog/2015/10/intermediary-liability-and-user-content-under-europe%E2%80%99s-new-data-protection-law

[5] http://cyberlaw.stanford.edu/blog/2015/10/gdpr%E2%80%99s-notice-and-takedown-rules-bad-news-free-expression-not-beyond-repair

[6] https://cyberlaw.stanford.edu/blog/2015/10/notice-and-takedown-under-gdpr-operational-overview

provides law students and the general public with educational resources and analyses of policy issues arising at the intersection of law, technology and the public interest. CIS also sponsors a range of public events including a speakers series, conferences and workshops. CIS was founded by Lawrence Lessig in 2000.

Response to Questions for the Record from Ambassador Peter Allgeier, President, Coalition of Service Industries (CSI)

Questions for the Record from Representative Ted Poe (TX-02) for Ambassador Peter Allgeier, President, Coalition of Service Industries

Question 1:

The German DPA has focused on US companies doing business in Germany, and highlighted that such US companies might be prohibited from transferring data to the US, as part of their cross-border business. I would like to understand whether the same prohibition would apply to German headquartered companies that are involved in substantial cross-border business and investment in the US. Many of which use the same global business models as US companies, and all of which are equally subject to US government laws when doing business here. I want to ensure I understand the potential trans-Atlantic economic impact, and not only the impact to US companies. Given this, do you know whether the same German DPA prohibition on data transfer would apply to German companies that operate in both countries? DHL, Deutsche Bank, Allianz, Deutsche Telekom/T-Mobile for example? Do they not need to send some German personal data to their US offices as part of commerce?

Question 2:

The ECJ and German conclusions that the US conducts "massive and indiscriminate surveillance" of communications appears to be the focus of the prohibitions on data transfer Setting aside for now any debate about the accuracy of the ECJ's characterization of data protection in the US, it seems that the focus of these limits on e-commerce is exclusively on the US. However, there is wide spread awareness that many countries have national security surveillance mandates. There are also studies that highlight the existence in many countries of sweeping mandates that lack procedural safeguards found in the US. But the ECJ and Germany solely focus on the US, and I want to better understand if there is a risk here of economic discrimination. Is there any indication that German officials would prohibit data transfers to France or the UK, which are EU Member States, but known to have expansive legal powers for surveillance? Is there any indication that German officials will apply these restrictions to German companies that operate in Russia or China, or to Russian and Chinese companies that operate in Germany? I have not heard discussion about potential EU or German restrictions in any of these instances, and it makes me worry about economic discrimination -- data protectionism dressed up as data protection.

Questions for the Record from Representative Ted Poe (TX-02) for Ambassador Peter Allgeier, President, Coalition of Service Industries

Response:

1. The U.S. – EU Safe Harbor Framework was negotiated to establish certification for U.S companies' processing of data of EU citizens under certain principles and guidelines. This was instituted to facilitate business of U.S. companies in the EU while maintaining EU standards of privacy and data protection. The annulment of Safe Harbor removes this certification for U.S. companies, and only pertains to their ability to move data from Europe to the United States. While German companies transferring data must still meet EU privacy standards by abiding by the EU Commission's Binding Corporate Rules (BCR) protecting private data, they are unaffected by the removal of Safe Harbor for U.S. companies.

2. Regardless of country-specific surveillance characteristics, common EU rules have been established to ensure that personal data enjoys a consistent standard of protection everywhere in the EU. This unified measure was put in place to prevent disruption that would accompany differing data protection rules between EU member states. While EU citizens have channels to complain if they feel their data was misused, it is unlikely German officials would, or would be able to broadly prevent data transfers to another EU member state. The EU does not have a Safe Harbor agreement in place with either Russia or China, so any data transfers to and from those countries would be governed uniformly under the EU Binding Corporate Rules. The annulment of Safe Harbor with the U.S. means that the U.S. loses its privileged status, relatively speaking, with regard to managing EU private data, and operates with the same restrictions placed on all non-EU member states.

Response to Questions for the Record from Robert D. Atkinson, Ph.D., Founder and President, The Information Technology and Innovation Foundation

ITIF | INFORMATION TECHNOLOGY & INNOVATION FOUNDATION

Response to questions from Representative Ted Poe from November 3rd House Judiciary hearing on "International Data Flows.

Robert Atkinson
President, Information Technology and Innovation Foundation
December 14, 2015

1) Will the German DPA prohibition on data transfers from U.S. companies doing business in Germany to the U.S. also apply to German companies in Germany?

My understanding is that the under the EU privacy directive, the nationality of the company in the EU is irrelevant to the rules governing data transfer. As such if a German company wanted to move data containing personally identifiable information on a person in Germany to an affiliate in the U.S. they would need to use other legal means, such as binding corporate rules.

2) Does the EU policy re U.S. government surveillance amount to economic discrimination?

Yes, the focus of the ECJ and German DPA appear to be only on the risk of inappropriate surveillance in the United States and not other nations. And as such this appears to be a case of economic discrimination. For example, while the ECJ has invalidated the Safe Harbor agreement with the United States on the grounds that EU citizen data is not safe from government access, it still maintains that other nations with similar laws and practices provide adequate protection. If anything, EU citizen data is safer from government access in the United States than it is in nations like Argentina and Israel, yet European privacy authorities and courts have not revoked data sharing agreements with either of those nations. Moreover, there are reports that the German intelligence agency BND had "systemically" spied on citizens from Denmark, France, Great Britain, Italy, and Sweden. But there has been no action by affected nations to limit data flows to companies in Germany. On Danish politician commented "Everyone spies on everyone. That's what they do. There is nothing odious in it. I would be very disappointed if we didn't also do it to our other friends."[1] So the message is that EU nations can "spy" on citizens of other EU nation without any effect on rules governing cross-border data transfer within the EU, but the U.S. government is singled out. Likewise, the German DPA has shown no signs that it wants to limit the transfer of German person data to other nations, such as France or UK, where government surveillance practices are similar to the U.S.

[1] http://www.thelocal.dk/20151109/denmark-to-do-nothing-about-alleged-germany-spying

Response to Questions for the Record from Victoria Espinel, President and CEO, BSA | The Software Alliance



Answers to the Questions for the Record from Representative Ted Poe (TX-02):

Question 1:

The German DPA has focused on US companies doing business in Germany, and highlighted that such US companies might be prohibited from transferring data to the US, as part of their cross-border business. I would like to understand whether the same prohibition would apply to German headquartered companies that are involved in substantial cross-border business and investment in the US. Many of which use the same global business models as US companies, and all of which are equally subject to US government laws when doing business here. I want to ensure I understand the potential trans-Atlantic economic impact, and not only the impact to US companies. Given this, do you know whether the same German DP A prohibition on data transfer would apply to German companies that operate in both countries? DHL, Deutsche Bank, Allianz, Deutsche Telekom/T-Mobile for example? Do they not need to send some German personal data to their US offices as part of commerce?

Answer:

Without addressing the practices of any specific company, the straightforward answer to this question is this: European privacy law generally prohibits the transfer of data outside the EU unless an adequate level of protection is guaranteed by the laws of the country where the data is to be sent. Data protection, however, is not a straightforward area of the law. And certain exceptions to this rule exist that would allow a German company to transfer the personal data of its customers or employees to the United States.

For example, the intra-company transfer of data across borders can be performed subject to binding corporate rules (BCRs). BCRs allow multinational companies, organizations, and groups to facilitate international transfers of personal data, while ensuring that the transfers comply with EU data protection laws. Alternatively, companies can use EU-approved model contract clauses for certain categories of data transfers.

Given these other mechanisms, a German company could transfer data to the United States – or to another country that has not been deemed "adequate" by the European Union – so long as the company itself is deemed to be providing the proper levels of data protection.

Question 2:

The ECJ and German conclusions that the US conducts "massive and indiscriminate surveillance" of communications appears to be the focus of the prohibitions on data transfer. Setting aside for now any debate about the accuracy of the ECJ' s characterization of data protection in the US, it seems that the focus of these limits on e-commerce is exclusively on the US. However, there is wide spread awareness that many countries have national security surveillance mandates. There are also studies that highlight the existence in many countries of sweeping mandates that lack procedural safeguards found in the US. But the ECJ and Germany solely focus on the US, and I want to better understand if there is a risk here of economic discrimination. Is there any indication that German officials would prohibit data · transfers to France or the UK, which are EU Member States, but known to have expansive legal powers for

20 F Street, NW, Suite 800
Washington, DC 20001
P 202-872-5500
W bsa.org

surveillance? Is there any indication that German officials will apply these restrictions to German companies that operate in Russia or China, or to Russian and Chinese companies that operate in Germany? I have not heard discussion about potential EU or German restrictions in any of these instances, and it makes me worry about economic discrimination -- data protectionism dressed up as data protection.

Answer:

The European Data Protection Directive sets the standard privacy regime across the Member States of the European Union. Under that regime, data transfers are enabled throughout the Union. This is true even though the views on data privacy and surveillance are not identical across all Member States. While there have been some reported incidents of German data protection authorities questioning transfers to other EU Member States, we are not aware of any serious indications that German officials would prohibit data transfers to France or the United Kingdom.

As it relates to restrictions on German companies' ability to restrict data transfers to Russia or China, or the transfer of data by Russian or Chinese companies that operate in Germany, such transfers could only occur under EU-approved Binding Corporate Rules or other data transfer mechanisms, as allowed by the EU Data Protection Directive.

Question 3:

Given the ECJ concern about alleged mass surveillance that it contends exists in the US and the limits on European citizens to seek redress of their privacy rights in the US, could you think these concerns would dissipate if and when (1) bulk data collection ends in December pursuant to the terms of the PATRIOT Act reauthorization; and (2) if the Judicial Redress Act is adopted as law?

Answer:

It is our hope that there will be a reduction in concerns as the USA Freedom Act reforms are put in place. BSA member companies supported this legislation as well as the House-passed Judicial Redress Act, which we hope the Senate will soon pass. We believe these bills are critical to demonstrating the importance that the United States places on privacy, and we thank the members of the House for their support.

Despite this hard work, the fact remains that, while both the US and the EU highly value privacy, the US and EU do have different approaches to privacy regulation. This does not mean that there is not a path forward to restore trust in a Safe Harbor system. It is critical that the US and EU continue to negotiate an updated Safe Harbor Framework to enable the normalization of data transfers between the US and EU.

To this end, the Commerce Department and Federal Trade Commission already have taken steps to improve the Safe Harbor system. These efforts included increased resources for the operation of the Safe Harbor within Commerce and recent enforcement actions against companies that were improperly claiming Safe Harbor certification.

20 F Street, NW, Suite 800
Washington, DC 20001

P 202-872-5500
W bsa.org

Response to Questions for the Record from Ed Black, President & CEO, The Computer & Communications Industry Association

BOB GOODLATTE, Virginia
CHAIRMAN

JOHN CONYERS, JR., Michigan
RANKING MEMBER

ONE HUNDRED FOURTEENTH CONGRESS

Congress of the United States

House of Representatives

COMMITTEE ON THE JUDICIARY

2138 RAYBURN HOUSE OFFICE BUILDING

WASHINGTON, DC 20515–6216

(202) 225–3951

http://www.house.gov/judiciary

November 19, 2015

Mr. Ed Black
President and CEO
Computer & Communications Industry Association
900 17th Street, NW, Suite 1100
Washington, D.C. 20006

Dear Mr. Black,

The Committee on the Judiciary's Subcommittee on Courts, Intellectual Property, and the Internet held a hearing on "International Data Flows: Promoting Digital Trade in the 21st Century" on Tuesday, November 3, 2015 in room 2141 of the Rayburn House Office Building. Thank you for your testimony.

Questions for the record have been submitted to the Committee within five legislative days of the hearing. The questions addressed to you are attached. We will appreciate a full and complete response as they will be included in the official hearing record.

Please submit your written answers to the Subcommittee by Thursday, December 31, 2015. Please send them via email or postal mail to the Committee on the Judiciary, Attention: Eric Bagwell, 6310 O'Neill Federal Building, Washington, DC, 20515. If you have any further questions or concerns, please contact Eric Bagwell on my staff at (202)-225-5741 or by email: Eric.Bagwell@mail.house.gov.

Thank you again for your participation in the hearing.

Sincerely,

Bob Goodlatte

Bob Goodlatte
Chairman

Enclosure

Questions for the record from Representative Ted Poe (TX-02):

Question 1:

The German DPA has focused on US companies doing business in Germany, and highlighted that such US companies might be prohibited from transferring data to the US, as part of their cross-border business. I would like to understand whether the same prohibition would apply to German headquartered companies that are involved in substantial cross-border business and investment in the US. Many of which use the same global business models as US companies, and all of which are equally subject to US government laws when doing business here. I want to ensure I understand the potential trans-Atlantic economic impact, and not only the impact to US companies. Given this, do you know whether the same German DPA prohibition on data transfer would apply to German companies that operate in both countries? DHL, Deutsche Bank, Allianz, Deutsche Telekom/T-Mobile for example? Do they not need to send some German personal data to their US offices as part of commerce?

Question 2:

The ECJ and German conclusions that the US conducts "massive and indiscriminate surveillance" of communications appears to be the focus of the prohibitions on data transfer. Setting aside for now any debate about the accuracy of the ECJ's characterization of data protection in the US, it seems that the focus of these limits on e-commerce is exclusively on the US. However, there is wide spread awareness that many countries have national security surveillance mandates. There are also studies that highlight the existence in many countries of sweeping mandates that lack procedural safeguards found in the US. But the ECJ and Germany solely focus on the US, and I want to better understand if there is a risk here of economic discrimination. Is there any indication that German officials would prohibit data transfers to France or the UK, which are EU Member States, but known to have expansive legal powers for surveillance? Is there any indication that German officials will apply these restrictions to German companies that operate in Russia or China, or to Russian and Chinese companies that operate in Germany? I have not heard discussion about potential EU or German restrictions in any of these instances, and it makes me worry about economic discrimination -- data protectionism dressed up as data protection.

Questions for the Record from Representative Ted Poe (TX-02) for
Mr. Ed Black, President and CEO, Computer & Communications Industry Association

Response to Question 1:

Representative Poe, thank you for your question. We share your concerns whether international companies headquartered in Europe, including those based in Germany, would be affected by an enforced prohibition on transatlantic transfers of EU data.

To the extent that German multinational companies, via their U.S.-based subsidiaries, relied on the Safe Harbor framework, they too would lack a legal basis to lawfully transfer personal data from the EU to the United States. Those companies share CCIA's concern over the ongoing legal uncertainty that all companies operating across the Atlantic currently face. For example, SAP, a German multinational enterprise software and services company with numerous clients on both sides of the Atlantic, has called for a new version of the Safe Harbor agreement to create "a distinct and reliable framework for transatlantic data traffic"—one that is uniform, reliable, predictable, and does not isolate Europe from the rest of the world.[1]

Many EU-based multinational companies take advantage of other mechanisms for EU law-compliant transatlantic data transfers, namely binding corporate rules and model contract clauses. However, those legal tools are now also under review by data protection authorities in the EU, including Hamburg, Germany's local data protection authority.[2] Should those mechanisms be declared invalid, even those EU-based companies that did not rely on the Safe Harbor framework for their transatlantic data flows will lack a clear legal basis to continue transfers.

Response to Question 2:

Representative Poe, thank you for your question. There have been no indications that German officials would prohibit data transfers to other EU Member States or third countries, like Russia or China, on the basis of expansive surveillance authorities in those countries.

This is the case for two reasons. First, at present, the only data transfer mechanism that has been invalidated by the Court of Justice of the European Union (CJEU) is the EU-U.S. Safe Harbor framework. While the court's rationale in the *Schrems* judgment regarding the breadth of national security exceptions in third country data transfer instruments could likely be extended to

---

[1] Press Release, *SAP Statement on the ECJ Decision on Safe Harbor*, Oct. 7, 2015, *available at* http://news.sap.com/sap-statement-on-the-ecj-decision-on-safe-harbor/.
[2] Christoph Ritzer, *et al.*, *German Data Protection Authorities Suspend BCR approvals, question Model Clause transfers*, Data Protection Report, Oct. 26, 2015, *available at* http://www.dataprotectionreport.com/2015/10/germandata-protection-authorities-suspend-bcr-approvals-question-model-clause-transfers/.

the instruments providing the basis for transfers to countries like Russia and China, a challenge to those tools has not been brought yet and they remain valid until ruled upon by the CJEU.

Second, while EU member states may have their own expansive surveillance authorities, there is little ability for, say, a German data protection authority to challenge data flows to France or the UK on the basis of EU-level legislation. The CJEU and other EU-level organizations generally do not have complete competence to rule on the national security activities of member states, and to the extent that they do, there is no pressure on individual member states to comply.[3] The European Parliament has recently voiced concern with surveillance programs in individual EU member states,[4] but it too has little influence on domestic activities of member states.

[3] *See* Christopher Wolf and Winston Maxwell, *Why the U.S. Is Held to a Higher Data Protection Standard Than France*, IAPP Privacy Perspectives, Nov. 2, 2015, *available at* https://iapp.org/news/a/why-the-u-s-is-held-to-a-higher-data-protection-standard-than-france/.

[4] Follow-up to the European Parliament resolution of 12 March 2014 on the electronic mass surveillance of EU citizens, P8_TA(2015)0388, Oct. 29, 2015, *available at* http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//TEXT+TA+P8-TA-2015-0388+0+DOC+XML+V0//EN.

Response to Questions for the Record from Mark MacCarthy, Senior Vice President, Public Policy, Software & Information Industry Association

Questions for the Record from Representative Ted Poe (TX-02) and
Answers from SIIA Senior Vice President for Public Policy, Mark MacCarthy:

Question 1:

The German DPA has focused on US companies doing business in Germany, and highlighted that such US companies might be prohibited from transferring data to the US, as part of their cross-border business. I would like to understand whether the same prohibition would apply to German headquartered companies that are involved in substantial cross-border business and investment in the US. Many of which us the same global business models as US companies, and all of which are equally subject to US government laws when doing business here. I want to ensure I understand the potential trans-Atlantic economic impact, and not only the impact to US companies. Given this, do you know whether the same German DPA prohibition on data transfer would apply to German companies that operate in both countries? DHL, Deutsche Bank, Allianz, Deutsche Telekom/T-Mobile for example? Do they not need to send some German personal data to their offices as part of commerce?

Answer 1:

Our understanding is that any transfer of personal identifiable information (PII) regarding German citizens from Germany to the United States, irrespective of the nationality of the company, would be covered by the prohibition. We do not know whether the companies mentioned in the question need to transfer some German personal data to their U.S. offices as part of commerce, although we think it is likely that many of these firms do so. The Future of Privacy Forum reports that there are more than 150 European companies that are participants in the U.S.-EU Safe Harbor Framework. Some of those companies are German such as Adidas, BMW, Bayer, Software AG, and Bertelsmann. These firms presumably have an interest in a new Safe Harbor Framework that would allow them to continue to transfer data to the United States.

Question 2:

The ECJ and German conclusions that the US conducts "massive and indiscriminate surveillance" of communications appears to be the focus of the prohibitions on data transfer. Setting aside for now any debate about the accuracy of the ECJ's characterization of data protection in the US, it seems that the focus of these limits on e-commerce is exclusively on the US. However, there is wide spread awareness that many countries have national security surveillance mandates. There are also studies that highlight the existence in many countries of sweeping mandates that lack procedural safeguards found in the US. But the ECJ and Germany solely focus on the US, and I want to better understand if there is a risk here of economic discrimination. Is there any indication that German Officials would prohibit Data transfers to France or the US, which are EU Member States, but known to have expansive legal powers for surveillance? Is there any indication that German officials will apply these restrictions to German companies that operate in Russia or China, or to Russian and Chinese companies that operate in Germany? I have not heard discussion about potential EU or German restrictions in any of these instances, and it makes me worry about economic discrimination – data protectionism dressed up as data protection.

Answer 2:

SIIA is not aware of whether German officials might prohibit data transfer to the UK or France. SIIA has no information on whether German officials might apply data flow restrictions to German companies that operate in Russia or China or to Russian or Chinese companies that operate in Germany. We agree with your assessment that many countries have national security mandates and some of them lack the procedural safeguards found in the U.S. SIIA's view on whether there is economic discrimination is that whatever the motive or legal reasoning is for restricting data flows, there is an economic cost. Ultimately that cost is borne by consumers. Moreover, restrictions on data flows undermine the concept of one open Internet, which the European Union and European countries say they support.

Question 3:

Given the ECJ concern about alleged mass surveillance that it contends exist in the US and the limits on European citizens to seek redress of their privacy rights in the US, do you think these concerns would dissipate if and when (1) bulk collection ends in December pursuant to the terms of the PATRIOT Act reauthorization; and (2) if the Judicial Redress Act is adopted as law?

Answer 3:

As you know, the USA FREEDOM Act, enacted into law earlier this year, made significant reform to Section 215 of the PATRIOT Act regarding bulk collection of Americans' telephone records and Internet metadata. The USA FREEDOM Act effectively banned the bulk collection of data, beginning December, 2015, by requiring specific criteria for government access to these records. We believe that this change and other changes presented by the USA FREEDOM Act should go a long way towards alleviating concerns of foreign governments and the European Court of Justice (ECJ) that the broad authority provided under Section 215 could be extended to include call records and data from non-American citizens and foreign businesses.

We also believe that the enactment of the Judicial Redress Act would help to alleviate concerns of foreign governments, particularly those stemming from the EU and the recent ECJ decision. European officials have indicated that providing European citizens with limited remedies similar to those Americans enjoy under the Privacy Act is a critical element to providing adequate privacy rights to European citizens. The JRA represents a leveling of the playing field of sorts, as U.S. citizens currently have redress rights to ensure the accuracy of data held about them in most EU member states.

○