

**21ST CENTURY TRADE BARRIERS: PROTECTIONIST  
CROSS BORDER DATA FLOW POLICIES IMPACT  
ON U.S. JOBS**

---

**HEARING**  
BEFORE THE  
SUBCOMMITTEE ON DIGITAL COMMERCE AND  
CONSUMER PROTECTION  
OF THE  
COMMITTEE ON ENERGY AND  
COMMERCE  
HOUSE OF REPRESENTATIVES  
ONE HUNDRED FIFTEENTH CONGRESS  
FIRST SESSION

OCTOBER 12, 2017

**Serial No. 115-66**



Printed for the use of the Committee on Energy and Commerce  
*energycommerce.house.gov*

U.S. GOVERNMENT PUBLISHING OFFICE

27-652

WASHINGTON : 2018

---

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 ENERGY AND COMMERCE

GREG WALDEN, Oregon

*Chairman*

JOE BARTON, Texas

*Vice Chairman*

FRED UPTON, Michigan

JOHN SHIMKUS, Illinois

TIM MURPHY, Pennsylvania

MICHAEL C. BURGESS, Texas

MARSHA BLACKBURN, Tennessee

STEVE SCALISE, Louisiana

ROBERT E. LATTA, Ohio

CATHY McMORRIS RODGERS, Washington

GREGG HARPER, Mississippi

LEONARD LANCE, New Jersey

BRETT GUTHRIE, Kentucky

PETE OLSON, Texas

DAVID B. MCKINLEY, West Virginia

ADAM KINZINGER, Illinois

H. MORGAN GRIFFITH, Virginia

GUS M. BILIRAKIS, Florida

BILL JOHNSON, Ohio

BILLY LONG, Missouri

LARRY BUCSHON, Indiana

BILL FLORES, Texas

SUSAN W. BROOKS, Indiana

MARKWAYNE MULLIN, Oklahoma

RICHARD HUDSON, North Carolina

CHRIS COLLINS, New York

KEVIN CRAMER, North Dakota

TIM WALBERG, Michigan

MIMI WALTERS, California

RYAN A. COSTELLO, Pennsylvania

EARL L. "BUDDY" CARTER, Georgia

FRANK PALLONE, JR., New Jersey

*Ranking Member*

BOBBY L. RUSH, Illinois

ANNA G. ESHOO, California

ELIOT L. ENGEL, New York

GENE GREEN, Texas

DIANA DeGETTE, Colorado

MICHAEL F. DOYLE, Pennsylvania

JANICE D. SCHAKOWSKY, Illinois

G.K. BUTTERFIELD, North Carolina

DORIS O. MATSUI, California

KATHY CASTOR, Florida

JOHN P. SARBANES, Maryland

JERRY McNERNEY, California

PETER WELCH, Vermont

BEN RAY LUJAN, New Mexico

PAUL TONKO, New York

YVETTE D. CLARKE, New York

DAVID LOEBSACK, Iowa

KURT SCHRADER, Oregon

JOSEPH P. KENNEDY, III, Massachusetts

TONY CARDENAS, California

RAUL RUIZ, California

SCOTT H. PETERS, California

DEBBIE DINGELL, Michigan

## SUBCOMMITTEE ON DIGITAL COMMERCE AND CONSUMER PROTECTION

ROBERT E. LATTA, Ohio

*Chairman*

GREGG HARPER, Mississippi

*Vice Chairman*

FRED UPTON, Michigan

MICHAEL C. BURGESS, Texas

LEONARD LANCE, New Jersey

BRETT GUTHRIE, Kentucky

DAVID B. MCKINLEY, West Virginia

ADAM KINZINGER, Illinois

GUS M. BILIRAKIS, Florida

LARRY BUCSHON, Indiana

MARKWAYNE MULLIN, Oklahoma

MIMI WALTERS, California

RYAN A. COSTELLO, Pennsylvania

GREG WALDEN, Oregon (*ex officio*)

JANICE D. SCHAKOWSKY, Illinois

*Ranking Member*

BEN RAY LUJAN, New Mexico

YVETTE D. CLARKE, New York

TONY CARDENAS, California

DEBBIE DINGELL, Michigan

DORIS O. MATSUI, California

PETER WELCH, Vermont

JOSEPH P. KENNEDY, III, Massachusetts

GENE GREEN, Texas

FRANK PALLONE, JR., New Jersey (*ex*

*officio*)

## CONTENTS

---

	Page
Hon. Robert E. Latta, a Representative in Congress from the State of Ohio, opening statement .....	1
Prepared statement .....	3
Hon. Janice D. Schakowsky, a Representative in Congress from the State of Illinois, opening statement .....	4
Hon. Michael C. Burgess, a Representative in Congress from the State of Texas, opening statement .....	5
Hon. Frank Pallone, Jr., a Representative in Congress from the State of New Jersey, prepared statement .....	80
WITNESSES	
Victoria A. Espinel, President and CEO, BSA—The Software Alliance .....	6
Prepared statement .....	9
Answers to submitted questions .....	88
Dean C. Garfield, President and CEO, Information Technology Industry Council .....	22
Prepared statement .....	24
Answers to submitted questions .....	90
Jennifer Daskal, Associate Professor of Law, American University Wash- ington College of Law .....	41
Prepared statement .....	43
Morgan Reed, President, ACT—The App Association .....	53
Prepared statement .....	55
Answers to submitted questions .....	93
SUBMITTED MATERIAL	
Statement of the Insights Association .....	81
Statement of the Electronic Privacy Information Center .....	83



## **21ST CENTURY TRADE BARRIERS: PROTECTIONIST CROSS BORDER DATA FLOW POLICIES IMPACT ON U.S. JOBS**

**THURSDAY, OCTOBER 12, 2017**

HOUSE OF REPRESENTATIVES,  
SUBCOMMITTEE ON DIGITAL COMMERCE AND CONSUMER  
PROTECTION,  
COMMITTEE ON ENERGY AND COMMERCE,  
*Washington, DC.*

The subcommittee met, pursuant to call, at 10:17 a.m., in room 2322, Rayburn House Office Building, Hon. Robert Latta, (chairman of the subcommittee) presiding.

Present: Representatives Harper, Burgess, Lance, Guthrie, Bilirakis, Mullin, Walters, Costello, Schakowsky, Clarke, Dingell, Matsui, Welch, Kennedy, Green, and Latta.

Staff Present: Zachary Dareshori, Staff Assistant; Melissa Froelich, Chief Counsel, Digital Commerce and Consumer Protection; Adam Fromm, Director of Outreach and Coalitions; Ali Fulling, Legislative Clerk, Oversight and Investigations, Digital Commerce and Consumer Protection; Theresa Gambo, Human Resources/Office Administrator; Elena Hernandez, Press Secretary; Paul Jackson, Professional Staff, Digital Commerce and Consumer Protection; Bijan Koohmaraie, Counsel, Digital Commerce and Consumer Protection; Madeline Vey, Policy Coordinator, Digital Commerce and Consumer Protection; Greg Zerzan, Counsel, Digital Commerce and Consumer Protection; Michelle Ash, Minority Chief Counsel, Digital Commerce and Consumer Protection; Lisa Goldman, Minority Counsel; and Caroline Paris-Behr, Minority Policy Analyst.

### **OPENING STATEMENT OF HON. ROBERT E. LATTA, A REPRESENTATIVE IN CONGRESS FROM THE STATE OF OHIO**

Mr. LATTA. Well, good morning. I would like to call the Subcommittee on Digital Commerce and Consumer Protection to order. And the chair now recognizes himself for 5 minutes for an opening statement.

And good morning again. I appreciate our witnesses for being with us today for this important hearing on digital trade and international data flows and the impact on U.S. industry. The free transmission of data across borders contributes to a seamless exchange of information, goods, and services. Digital trade has been a significant benefit to the U.S. economy, contributing an estimated

2.4 million new jobs, raising real U.S. GDP, and exceeding the economic trade value of traditional goods and services.

Today, we will hear from our witnesses about the current state of digital economy and its positive impact on U.S. competition, job creation, and economic growth. I hope that this hearing will be a jumping off point for a closer examination of these and other non-tariff trade matters in the months to come.

What is digital trade? It happens in each and every one of our daily lives when we use our personal laptops, tablets, smartphones, or when companies work to complete projects for customers. While this might seem broad and difficult to define, one of our witnesses today, Mr. Garfield, puts forward a clean definition: Digital trade is simply an economic activity involving the movement of digital information across borders.

At the enterprise level, companies might be using services and applications like cloud computing, data processing, and predictive analytics. Uses can include processing payroll or designing products that are easy to manufacture at the highest quality possible for the lowest price.

Through our work already this year, this committee has heard from many companies using the power of data flows to improve public policy goals like improving passenger safety and mobility, access through self-driving car technology. The internet, data, and digital trade now support economic growth in all sectors of the U.S. economy. U.S. industry around the country, whether in manufacturing, retail, and energy, and healthcare rely on cross-border data flows to run their businesses. This technological phenomenon also supports local businesses and smaller enterprises, including entrepreneurs and app developers.

According to a study by eBay, over 90 percent of eBay U.S. businesses trade across borders with more than 80 percent reaching five or more international markets. These small to medium-size companies touch all States and congressional districts.

In my home State of Ohio, the software industry directly employs over 72,000 people and was responsible for \$11 billion in direct value-added GDP in 2014. In my district, there are over 38,000 high-tech workers in exports of digital goods and services totaling over \$690 million in 2014.

While these numbers are a few years old, in my visits to businesses around my district, I have certainly seen the impact of high-skilled workers in the manufacturing industries. Despite the many benefits of cross-border data flows, many trading partners have considered or adopted nontariff barriers, such as restrictions on cross-border data flows or requirements to localize data, production, or facilities.

If the internet is characterized by openness, then data localization and other data flow restrictions create conflict either intentionally as a protectionist measure or unintentionally. The witnesses here today can speak about the data localization measures in force and the potential spread of additional restrictions. I am very pleased to hear about how the impact of these policies on businesses in my district are affected and around the country.

Last year, the European Union and the United States put into place the EU-U.S. Privacy Shield. And last month, the European

Commission began its first review of the Privacy Shield. In 1 year, the Privacy Shield has been embraced by over 2,500 U.S. companies of all sizes and business models to allow for the free flow of data between the EU and the United States.

Finally, there are multiple trade negotiation dialogues that are expected to set the stage for digital trade and data flow policy moving forward. Current trade agreements were written before the advent of the internet as we know it today. Going forward, there is a tremendous potential for the digital economy as we consider cross-border data flow policies and robust enforcement measures.

We are living in an extraordinary time of growth in today's digitally integrated global economy. The impact of digital trade and cross-border data flows will reach far and wide, and I believe Congress can play a significant role in supporting the people and businesses that depend on the free and open flow of data. I look forward to hearing from our witnesses today on this very timely matter.

And at this time, I would like to recognize the ranking member of the subcommittee, the gentlelady from Illinois, for 5 minutes for an opening statement.

[The prepared statement of Mr. Latta follows:]

#### PREPARED STATEMENT OF HON. ROBERT E. LATTA

Good morning. I appreciate our witnesses being here today for this important hearing on digital trade and international data flows, and the impact on U.S. industry.

The free transmission of data across borders contributes to a seamless exchange of information, goods, and services. Digital trade has been a significant benefit to the U.S. economy, contributing to an estimated 2.4 million new jobs, raising real U.S. GDP, and exceeding the economic trade value of traditional goods and services.

Today we will hear from our witnesses about the current state of the digital economy and its positive impact on U.S. competition, job creation, and economic growth. I hope that this hearing will be a jumping-off point for a closer examination of these and other non-tariff trade matters in the months to come.

What is digital trade? It happens in each and every one of our daily lives—when we use our personal laptops, tablets and smartphones, or when companies work to complete projects for customers.

While this might seem broad and difficult to define, one of our witnesses today, Mr. Garfield, puts forward a clean definition: “Digital trade is simply any economic activity involving the movement of digital information...across borders.”

At the enterprise level, companies might be using services and applications like cloud computing, data processing, and predictive analytics. Uses can include processing payroll or designing products that are easy to manufacture at the highest quality possible, for the lowest price.

Through our work already this year, this committee has heard from many companies using the power of data flows to improve public policy goals like improving passenger safety and mobility access through self-driving car technology.

The Internet, data, and digital trade now support economic growth in all sectors of the U.S. economy. U.S. industry around the country—whether in manufacturing, retail, energy, and health care—rely on “cross-border data flows” to run their businesses.

This technological phenomenon also supports local businesses and smaller enterprises including entrepreneurs and app developers. According to a study by eBay, over 90 percent of eBay's U.S. businesses trade across borders, with more than 80 percent reaching five or more international markets.

These small-to-medium sized companies touch all states and congressional districts. In my home State of Ohio, the software industry directly employed over 72,000 people, and was responsible for \$11 billion in direct value-added GDP in 2014.

In my district, there were over 38,000 high-tech workers and exports of digital goods and services totaled over \$690 million in 2014. While these numbers are a

few years old, in my visits to businesses around my district, I have certainly seen the impact of high-skilled workers in the manufacturing industry.

Despite the many benefits of cross border data flows, many trading partners have considered or adopted nontariff barriers, such as restrictions on cross-border data flows or requirements to localize data, production, or facilities.

If the Internet is characterized by openness, then data localization and other data flow restrictions create conflict—either intentionally, as a protectionist measure, or unintentionally.

The witnesses here today can speak about the data localization measures in force and the potential spread of additional restrictions. I am very interested to hear about the impact of these policies on businesses in my district and around the country.

Last year the European Union and United States put into place the EU-U.S. Privacy Shield and last month, the European Commission began its first review of the Privacy Shield. In one year, the Privacy Shield has been embraced by over 2,500 U.S. companies—of all sizes and business models—to allow for the free flow of data between the EU and the U.S.i

Finally, there are multiple trade negotiations and dialogues that are expected to set the stage for digital trade and data flow policy moving forward. Current trade agreements were written before the advent of the Internet as we know it today. Going forward, there is tremendous potential for the digital economy as we consider cross border-data flow policies and robust enforcement measures.

We are living in an extraordinary time of growth in today's digitally-integrated global economy. The impact of digital trade and cross-border data flows will reach far and wide, and I believe Congress can play a significant role in supporting the people and businesses that depend on the free and open flow of data. I look forward to hearing from our witnesses today about this timely issue.

#### **OPENING STATEMENT OF HON. JANICE D. SCHAKOWSKY, A REPRESENTATIVE IN CONGRESS FROM THE STATE OF ILLINOIS**

Ms. SCHAKOWSKY. Thank you, Chairman Latta.

The internet has made our world dramatically more connected than ever before. It facilitates the exchange of ideas, keeps families connected, and creates new opportunities for global commerce. Over 2.3 billion people have access to the internet, and this is expected to grow to 5 billion by 2020.

Digital commerce comprises a growing share of the global economy, and, in fact, a McKinsey report claims that, “soaring cross-border data flows now generate more economic value than traditional flows of traded goods.” Cross-border data flows allow for quick communication, whether it is a personal message or a customer order. It also introduces additional risks to consumers, privacy, and data security.

Global digital commerce has become a necessity in the United States economy. Although the internet is global, the rules governing data are not. Differences among countries can create challenges for businesses and consumers. Countries should not be dissuaded from protecting their citizens' privacy and security. But some of the policies we see across the world today are counterproductive to data security and privacy. Requiring local servers can create new security risks. The U.S. should also not empower regimes that monitor or restrict flow of data as a limit on their citizens' rights to free speech and expression.

We need to distinguish between policies that truly represent an unnecessary or harmful barrier to digital trade and those policies designed to protect privacy and security. When it comes to data privacy and security, current U.S. law is lacking. We heard a clear example of that last week when former Equifax CEO Richard Smith

testified in front of our committee. By failing to patch a known vulnerability, Equifax allowed the data of 145.5 million Americans to be compromised. I still have a lot of questions about this breach. Today, my Democratic colleagues and I are sending a letter to the majority requesting additional hearings to get answers that Americans deserve.

The Equifax breach impacted not only Americans, but also consumers outside the United States. So you can understand if consumers and governments abroad have their doubts about the data practices of American companies. This is yet another reason why we need to act in Congress to improve data security. And last week, I introduced the Secure and Protect Americans' Data Act to ensure that companies take sufficient steps to protect consumers' data and promptly notify law enforcement and consumers if a data breach occurs and provide meaningful relief to breach victims.

Digital trade partners are also concerned about U.S. surveillance practices. Section 702 expires at the end of this year, and we should take this opportunity to better protect privacy, while still providing for our Nation's security.

So as we strengthen our own laws, we need to continue engaging with partners, such as the European Union, on ways to facilitate cross-border data flows, while ensuring that consumers here and abroad enjoy the privacy and security they expect. The United States benefits greatly from digital trade, and we should work to keep data flowing across borders. That requires improving our own laws and engaging with other Nations on how to keep consumers' data and rights protected. I look forward to hearing from our witnesses and getting our perspective on this complex issue.

I yield back.

Mr. LATTA. Well, thank you very much. The gentlelady yields back.

And the chairman of the full committee is not here, but the gentleman from Texas would like to claim his time.

**OPENING STATEMENT OF HON. MICHAEL C. BURGESS, A  
REPRESENTATIVE IN CONGRESS FROM THE STATE OF TEXAS**

Mr. BURGESS. Thank you, Mr. Chairman, and thanks for holding the hearing. Thanks to our witnesses for being with us this morning.

In 2015, the European Court of Justice invalidated the United States-European Union Safe Harbor Framework. This subcommittee held hearings to evaluate the effect that this would have on trade, the risks to technological advancements, and the economic impact of this ruling. In the absence of an agreement, small and medium-sized businesses were certain to suffer, leading to decreased output and job losses. Almost a year later, the United States and the European Union approved the Privacy Shield Framework to replace the Safe Harbor and allow compliance with European Union data protection requirements.

Even though the Privacy Shield was approved, the United States is again facing restrictions that will decrease cross-border data flows and may even lead to actual data theft or theft of intellectual property or increased control of information flows. The free flow of data improves trade relations. It actually enhances technologies

like blockchain and artificial intelligence that rely on large datasets and improve security by increasing awareness of foreign activity, as well as providing redundancy for data through disaggregation.

In our interconnected world, it is imperative that concerns over privacy do not become protectionist. I certainly look forward to what our witnesses have to share with us today about how to safely and securely continue the advancements afforded by cross-data border flows.

And, again, Mr. Chairman, thank you for convening this hearing, and thanks again to our witnesses. And I will yield back my time.

Mr. LATTA. Well, thank you very much. The gentleman yields back.

And at this time, we will now move to our witnesses. We are concluding our members' statements. And pursuant to committee rules, all members will have their opening statements made part of the record.

And, again, I want to thank our witnesses for being with us today and taking time to testify before the subcommittee. And today's witnesses will have the opportunity to give a 5-minute opening statement, followed by a round of questions from our members.

Our witness panel today, for today's hearing, will include Ms. Victoria Espinel, the President and CEO of BSA, The Software Alliance; Mr. Dean Garfield, President and CEO of Information Technology Industry Council; Mr. Morgan Reed, President of ACT—The App Association; and Ms. Jennifer Daskal, Associate Professor of Law at American University Washington College of Law.

So I appreciate your being with us today.

And, Ms. Espinel, we will begin with you today. And just pull that mic up close and just turn the mic on. And we look forward to your testimony today. Thank you.

**STATEMENTS OF VICTORIA A. ESPINEL, PRESIDENT AND CEO, BSA—THE SOFTWARE ALLIANCE; DEAN C. GARFIELD, PRESIDENT AND CEO, INFORMATION TECHNOLOGY INDUSTRY COUNCIL; JENNIFER DASKAL, ASSOCIATE PROFESSOR OF LAW, AMERICAN UNIVERSITY WASHINGTON COLLEGE OF LAW; AND MORGAN REED, PRESIDENT, ACT—THE APP ASSOCIATION**

**STATEMENT OF VICTORIA A. ESPINEL**

Ms. ESPINEL. Thank you so much.

Good morning, Chairman Latta, Ranking Member Schakowsky, and members of the subcommittee. My name is Victoria Espinel, and I thank you for the opportunity to testify here today on behalf of BSA—The Software Alliance.

BSA members provide software-based services that have a significant positive impact on the U.S. economy and the global economy. Those services, such as cloud computing, data analytics, artificial intelligence, depend on the ability to transfer data freely across borders. As a result, eliminating barriers to cross-border data flows is an important priority for BSA and for our members, and I am very pleased that it is a priority for this committee as well.

When I testified before this committee 2 years ago, the U.S.-EU Safe Harbor agreement had just been invalidated by the European Court of Justice. The Safe Harbor agreement was a critical mechanism that allowed data to move back and forth between the United States and Europe, and, without it, transatlantic digital trade and the growth and job creation that go with it, on both sides of the Atlantic, would have been in jeopardy.

The bipartisan letter that was signed by the chairman and ranking member of the full committee and the subcommittee, and many other members of the committee, instilled much-needed confidence into the process, and the United States and the European Union were able to come to a conclusion of a new agreement, which has been called the Privacy Shield. And I thank the members of the committee for your leadership at that time. But I thank you as well for keeping continued focus on this issue, because we are continuing to see concerns around the world.

Our economy today is rooted in digital data. Across every industry sector cloud computing and data analysis have made businesses more agile, more responsive to their customer needs, and more competitive around the world. And all of these technologies depend on the ability to move data across borders.

So as an example, human resources is an important element of every company that exists. If you are a company that has employees across the United States, but also employees around the world, if you lack the ability to transfer that data about your employees back and forth, it will make it, among other things, much harder and much slower to hire and much harder and much slower to be able to reward your employees as you should. For U.S.-based companies, that also means that they will have less jobs in the United States because they will have to source and resource those functions overseas.

In cancer treatments, we are seeing great advances in artificial intelligence, allowing doctors to be able to make diagnoses more quickly and more accurately. And that is very dependent on the ability for doctors to be able to access as much data as possible about patients around the world.

In manufacturing, data around the world are allowing manufacturers to be much more responsive to their customer needs more quickly. And for small manufacturers in particular, that feedback loop to be able to get information from their customers and then be able to redesign their products to be more responsive to their customer needs is extremely important.

And what makes all of those examples work is the ability for data to move across borders. This is about real jobs and economic growth in the United States.

Last month, software.org, the BSA Foundation, released a study that we conducted with data from the Economist Intelligence Unit that shows that the software industry alone supports over 10 million jobs in the United States and significant jobs in every one of the 50 states of the United States. For example, since 2014, the number of software jobs has increased by nearly 10 percent in Ohio and by 14.4 percent in Illinois. Nationwide, softwares contributed \$1.14 trillion to the U.S. GDP and has grown at three times the speed of the overall economy.

U.S. leadership on digital trade will help ensure that this growth continues. We see three clear opportunities for Congress and the administration to act.

The first is to modernize the digital trade agenda. And, at the moment, NAFTA presents an opportunity for us to do that. When NAFTA was negotiated, the commercial internet essentially did not exist, digital trade was in its infancy, and, as a result, the agreement, understandably, does not address digital issues. So there is a clear opportunity. We were encouraged to see that the administration included digital trade and cross-border data flows in this negotiating the objectives. And we are very pleased that Congress has also included those in the objectives that they have set out for the administration to meet.

Second, ensure the continued success of the Privacy Shield. I alluded a moment ago to this committee's important role and the conclusion of the Privacy Shield. The Privacy Shield just had, last month, its first review. There are 2,500 companies that have already certified under it, as the chairman noted. And continuing to impart to both the U.S. administration and to the Europeans the importance of the Privacy Shield continuing is extremely important.

And the third thing I would suggest is to continue to encourage like-minded trading partners to promote rules that support the movement of data across borders, whether that is in formal trade negotiations or outside of formal trade negotiations. The U.S. is the leader in the technology that drives economic growth and depends on the ability for data to move across borders. We need the United States Government to also show leadership on this issue if we are to remain dominant in this area. And we know that if we do not, there are other countries that would be happy to move into that position.

So, with that, I will conclude my remarks. And thank you very much for continuing to focus on this issue.

[The prepared statement of Ms. Espinel follows:]



**Hearing on**

**“21<sup>st</sup> Century Trade Barriers: Protectionist Cross Border  
Data Flow Policies’ Impact on U.S. Jobs”**

**House Committee on Energy and Commerce  
Subcommittee on Digital Commerce  
and Consumer Protection**

**October 12, 2017, at 10:15 a.m.  
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 "21<sup>st</sup> Century Trade Barriers:**  
**Protectionist Cross Border Data Flow Policies' Impact on U.S. Jobs"**

**October 12, 2017**

**Washington, DC**

Good morning Chairman Latta, Ranking Member Schakowsky, and members of the Subcommittee. My name is Victoria Espinel, and I am the President and CEO of BSA | The Software Alliance.

BSA is the leading advocate for the global software industry in the United States and around the world.<sup>1</sup> Our members provide services that have a significant impact on the U.S. and global economy, and those services often depend on the ability to transfer data freely around the world. As a result, an important priority for BSA is promoting international trade by eliminating barriers to global data transfers. I commend the Subcommittee for holding a hearing on this important topic, and I thank you for the opportunity to testify on behalf of BSA.

When I testified before this Committee about international data transfers two years ago, the U.S.-EU Safe Harbor agreement had just been invalidated by the European Court of Justice, jeopardizing growth and job creation on both sides of the Atlantic. The Safe Harbor agreement was the critical mechanism that allowed data to be transferred between the EU and the United States. Without it, the many jobs that depend on transatlantic digital trade would have been in

---

<sup>1</sup> BSA's members include: Adobe, ANSYS, Apple, Autodesk, Bentley Systems, CA Technologies, CNC/Mastercam, DataStax, DocuSign, IBM, Microsoft, Oracle, salesforce.com, SAS Institute, Siemens PLM Software, Splunk, Symantec, Trimble Solutions Corporation, The MathWorks, Trend Micro and Workday.

jeopardy—and the development of new artificial intelligence (AI), analytics, and other tools would have been impeded.

This Committee played an important leadership role at that time. The bipartisan letter sent in October 2015 by the Chairmen and Ranking Members of the full Committee and this Subcommittee, as well as many members of this Subcommittee and others, instilled the needed confidence that the United States and EU would find an alternative mechanism—the Privacy Shield. I thank this Committee for its leadership and welcome its continued support of policy initiatives that promote global data flows.

#### **I. Economic and Social Impact of Software and Data-Driven Innovation**

Our economy today—and economic growth and job creation in the foreseeable future—are rooted in digital data. The dropping costs of data storage, alongside the acceleration of data-driven innovation by BSA member companies and others, have led to profound new uses of data by enterprises across the economy. In high-tech and low-tech industries alike, the analysis of data has made businesses more agile, responsive, and competitive, boosting the underlying productivity of many key pillars of our economy.

The sheer quantity of data available to fuel these developments is astounding. Indeed, the units with which we measure data are nearly unheard of in any other context: approximately 2 quintillion bytes of data (that's two followed by 18 zeros) are generated every day,<sup>2</sup> and every two years, we are doubling the rate at which data is produced. By 2021, global IP traffic will

---

<sup>2</sup> See BSA, *What's the Big Deal With Data?*, 7 (Oct. 2015), at [http://data.bsa.org/wp-content/uploads/2015/10/bsadatastudy\\_en.pdf](http://data.bsa.org/wp-content/uploads/2015/10/bsadatastudy_en.pdf).

reach 3.3 zettabytes per year—over three *trillion* gigabytes of data.<sup>3</sup>

The software industry, and BSA members in particular, are at the forefront of the development of cutting-edge technologies and services that will drive the data economy, such as predictive analytics, cloud computing, AI, and blockchain technologies. These technologies spur job creation and economic growth, provide significant benefits to businesses, and improve the quality of life for many Americans, as well as people around the globe. These benefits are likely to grow substantially in the coming years.

#### A. Data Services Are Creating Job and Economic Growth

The economic 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.<sup>4</sup>

Last month, Software.org: The BSA Foundation released a study conducted by the Economist Intelligence Unit (EIU) that showed the software industry alone contributed more than \$1.14 trillion to the U.S. GDP in 2016—a \$70 billion increase in the past two years.<sup>5</sup> The study also showed that the software industry is a powerful job creator, supporting over 10.5 million jobs,

<sup>3</sup> 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](http://www.cisco.com/c/en/us/solutions/collateral/service-provider/ip-ngn-ip-next-generation-network/white_paper_c11-481360.html).

<sup>4</sup> See BSA *What's the Big Deal With Data?*, *supra* n. 2, at 14. Notably, the potential of digital data to improve the healthcare system is substantial: some estimates predict that if the healthcare sector were to use data more effectively to drive efficiency and quality, the sector could save more than \$300 billion every year. See James Manyika et al., “Big Data: The Next Frontier for Innovation, Competition, and Productivity,” *McKinsey Global Institute* (May 2011), at [http://www.mckinsey.com/insights/business\\_technology/big\\_data\\_the\\_next\\_frontier\\_for\\_innovation](http://www.mckinsey.com/insights/business_technology/big_data_the_next_frontier_for_innovation).

<sup>5</sup> Software.org: The BSA Foundation, *The Growing \$1 Trillion Economic Impact of Software* (Sept. 2017), 5, available at [https://software.org/wp-content/uploads/2017\\_Software\\_Economic\\_Impact\\_Report.pdf](https://software.org/wp-content/uploads/2017_Software_Economic_Impact_Report.pdf).

with a significant impact on job and economic growth in each of the 50 states.<sup>6</sup>

B. Data Services Are Key to Growth Across Industry Sectors

Software and data-driven innovation are driving economic growth across virtually all industry sectors, as businesses are increasingly using software and cloud-enabled platforms. These platforms facilitate human resources management, virtual collaboration, sophisticated design and modeling, remote maintenance, and a variety of other business functions. This data analysis is occurring at the core of their businesses and helping define how businesses operate and the services they offer. Software increasingly not only underpins their products, but also their business processes.

Examples of how businesses are using data analysis to drive innovation and improve their competitiveness exist across the economy:

For instance, companies use cloud-based human resource management software to hire, support, and conduct performance management for a workforce of tens of thousands of people, who are often spread across numerous subsidiaries and affiliates.<sup>7</sup> Cloud-based solutions, such as those BSA members provide, increase HR functionality by providing real-time access to employee data worldwide, giving managers broad business insight across borders and business processes. By enabling powerful self-service tools available via a phone app, employing data analytics to give managers and HR departments more insight into their workforces, and enabling easy documentation and auditing of HR transactions, cloud-based HR systems

<sup>6</sup> *Id.*

<sup>7</sup> See Oracle, *Cummins Centralizes Key Customs and Compliance Processes to Minimize Supply Chain Risk*, at <http://www.oracle.com/us/corporate/customers/customersearch/cummins-1-qlm-2602121.html>; see also Workday, *Workday and Sanofi: Creating One Vision from Many*, at <https://www.workday.com/content/dam/web/en-us/documents/case-studies/workday-sanofi-case-study.pdf>.

increase efficiency and ease of use while reducing costs. They also improve security, as providers use their expertise to protect against cyberattacks and implement state of the art measures across the entire system through a unified approach to security.

In addition, software-enabled data analysis is also helping the financial sector detect payment card fraud. As companies increasingly use sophisticated data analytics tools to glean insight into consumers' purchasing patterns, they are better able to identify potentially fraudulent transactions around the globe, which harm both consumers and businesses.<sup>8</sup>

There are myriad examples across a wide swath of industries that underscore the significant impact of software-induced innovation.<sup>9</sup> Whether it is improving human resource management or detecting financial fraud, optimizing manufacturing production or enhancing transportation services, the impact of software is visible in every industry, in every state, and across the globe.

#### C. Data Services Offer Clear Societal Benefits and Improve Government Services

Data analytics and related software tools are not only delivering economic benefits across industry sectors, but are also contributing to public health, safety, and the social good. Indeed, innovative software products are empowering teachers with more effective educational tools,

---

<sup>8</sup> As an example, one leading technology company noted that it can detect and block online fraud attempts in five seconds on average, helping to reduce the losses attributed to online fraudsters by \$2.2 billion. See Pablo Hernandez, *CA Technologies Uses AI Tech to Combat Online Fraud*, eSecurityPlanet, May 4, 2017, available at <https://www.esecurityplanet.com/network-security/ca-technologies-uses-ai-tech-to-combat-online-fraud.html>.

<sup>9</sup> Indeed, data analysis is even cultivating agricultural growth. For example, U.S. companies use virtual simulation software to improve the quality and reliability of new tractor models, helping them build durable and resilient tractors that allow U.S. farmers to be more productive and competitive. See Siemens, *Agricultural Machinery Manufacturer Uses LMS Virtual.Lab to Increase Endurance Simulation*, available at [https://www.plm.automation.siemens.com/en/about\\_us/success/case\\_study.cfm?Component=222942&ComponentTemplate=1481](https://www.plm.automation.siemens.com/en/about_us/success/case_study.cfm?Component=222942&ComponentTemplate=1481). Software innovation has even helped improve dairy production. Cloud technology powers programs such as a cow-monitoring system that gives farmers constant information on the health of their cows, allowing them to boost milk production, smooth the calving process, and ensure healthier animals. See Microsoft, *Connected cows help farms keep up with the herd*, available at <https://news.microsoft.com/features/connected-cows-help-farms-keep-up-with-the-herd/>.

matching underprivileged families in developing countries with access to small business loans, and delivering dramatic improvements to medical diagnostics and patient care, including those with disabilities.

For example, artificial intelligence solutions, powered by data analysis, are at the heart of new devices and applications that improve the lives of people with disabilities, including helping people with vision-related impairments interpret and understand photos and other visual content, and even to navigate their physical surroundings.<sup>10</sup> This technology opens new possibilities for people with vision impairments to navigate their surroundings, giving them increased independence and greater ability to engage with their communities.

Artificial intelligence technologies also are enabling a cognitive computing system to analyze large volumes of data, including patient information and medical test results, to assist physicians in evaluating possible treatment options for cancer patients.<sup>11</sup>

Data analysis is also helping governments provide better services to their citizens. For instance, using software that uses predictive analytics, the New York City Fire Department is combining data from 7,500 individual data collection points pulled from 17 city agency data streams to predict which of New York City's 1 million buildings are at greatest risk for fires.<sup>12</sup> Charlotte, North Carolina, is harnessing smart city software and sensors to achieve a 20 percent

---

<sup>10</sup> For instance, Microsoft recently released an intelligent camera app that uses a smartphone's built-in camera functionality to describe to low-vision individuals the objects that are around them. See Microsoft, *Seeing AI*, available at <https://www.microsoft.com/en-us/seeing-ai/>.

<sup>11</sup> IBM, *Watson for Oncology*, <https://www.ibm.com/watson/health/oncology-and-genomics/oncology/>; see also Jo Cavollo, *How Watson for Oncology Is Advancing Personalized Patient Care*, The ASCO Post, June 25, 2017, available at <http://www.ascopost.com/issues/june-25-2017/how-watson-for-oncology-is-advancing-personalized-patient-care/>.

<sup>12</sup> See BSA | The Software Alliance, *The \$1 Trillion Economic Impact of Software* (June 2016), 8 available at <http://softwareimpact.bsa.org/>.

reduction in energy usage—saving millions of taxpayer dollars in the process.<sup>13</sup> And Chicago has deployed a city-wide network of 500 lamppost-mounted sensors to monitor air quality, using software to identify environmental issues like pest infestations that could be connected to the incidence of asthma.<sup>14</sup>

In brief, the power of software is transforming our world for the better.

## **II. Data Flows Are Critical to These Data Services and Continued Innovation**

These transformative technologies often rely on the ability to move data freely from one place to another and, in many instances, around the world. Without this ability, most data-analytics software applications that businesses use today simply could not function effectively. For example, most modern software applications do not operate fully in isolation on a single device; rather, they connect to other devices and remote data centers through a variety of online services. Although a software user often creates or receives data on his or her device, the processing of that data increasingly occurs elsewhere, oftentimes in locations miles or even continents away. The ability to transfer data around the world is essential to this structure.

In addition, AI applications, which use computational analysis of data to uncover patterns and draw inferences, depend on machine learning technologies that must ingest huge volumes of data, most often from a wide variety of sources. A language translation program, for example, cannot constantly improve its "understanding" of French without access to large volumes of French-language content—which may come from millions of search queries, mobile apps, databases, and other sources. The data for these AI systems may originate from many sources located in multiple jurisdictions, making it imperative that enterprises can transfer data freely

---

<sup>13</sup> *See id.*

<sup>14</sup> *See id.*

across borders. Therefore, rules that limit or prohibit such cross-border data transfers invariably limit the insights and other benefits that AI systems can provide.

Cybersecurity is another area where the ability to transfer data is critical. Cloud-based storage of data across multiple locations can improve data security by establishing redundant, geographically dispersed back-ups, which can help mitigate physical risks to data like natural disasters, and by eliminating single points of failure. Storing all information in a single location can increase security risks because it isolates data in a high-target “data honeypot”—increasing the stakes and potential consequences of a single breach. By contrast, distributing data storage across multiple locations compartmentalizes data sets, making it easier to contain a breach in one location and minimizing the risk—from either physical damage or cyber-attack—to the entire data set. The ability to transfer data across borders is often necessary to share information between these storage locations. Moreover, dispersed data storage can facilitate continuous, around-the-clock security monitoring and response, with security professionals working across multiple time zones. Requiring data and data centers to be localized within a single country can eliminate these advantages.

More broadly, the data analytics tools that BSA member customers and other companies are using to transform their businesses increasingly require unrestricted transfers of data. These tools often require picking out “needles in the haystack” by drawing meaningful inferences and connections within vast, unstructured datasets. For example, for multinational companies, the ability to collect and holistically analyze data on network analytics, employee technology usages, and data flows are critical to effective enterprise management—they enable a business to comprehensively examine their operations and supply chains. Digital trade restrictions that undermine this kind of technology could cripple enterprise operations.

### III. Opportunities to Facilitate Digital Trade and Data Flows

Data services, including data storage, data processing, and analytics, are the fastest growing elements of digital trade, and these services rely on the free flow of data across borders.

According to a 2016 McKinsey report, the amount of global data transfers has grown by a multiple of 45 since 2005 and is expected to surge in the next decade.<sup>15</sup>

This new digital data economy demands a globally recognized rules-based system for digital trade, establishing clear rules, rights, and protections.

We encourage the United States to lead on digital trade policies to ensure this tremendous economic growth will continue. If the United States fails to lead, other countries—with different priorities—will fill the gap.

We see three clear opportunities for Congress and the Administration to lead, promoting digital trade and ensuring the continued free flow of data: (1) modernizing NAFTA, (2) ensuring the continued success of the EU-U.S. Privacy Shield, and (3) strengthening relationships with other key trade partners.

#### A. Modernization of NAFTA

The digital economy has evolved significantly since NAFTA was originally concluded 25 years ago. When NAFTA was negotiated, digital trade was in its infancy, and there were relatively few services that were delivered digitally globally. It is therefore not surprising that the agreement

---

<sup>15</sup> James Manyika, Susan Lund, Jacques Bughin, Jonathan Woetzel, Kalin Stamenov, and Dhruv Dhingra, *Digital Globalization: The New Era of Global Flows*, McKinsey Global Institute (Feb. 2016), available at <http://www.mckinsey.com/business-functions/digital-mckinsey/our-insights/digital-globalization-the-new-era-of-global-flows>.

does not address many of the digital trade issues our modern economy now faces; quite simply, the innovations of the last two decades were not and could not have been anticipated. Indeed, since NAFTA was negotiated, the American software industry has moved from floppy disks and bulky desktop computing to mobile apps, cloud computing, smart devices, and data analytics. NAFTA must now be modernized to enable the digital economy to continue to develop. We urge the United States to negotiate a well-constructed and modern agreement, with 21<sup>st</sup> century digital trade obligations that will drive U.S. job creation, competitiveness, and innovation.<sup>16</sup>

In particular, NAFTA should prohibit measures that impose barriers to market access for e-commerce and digital trade. Perhaps most importantly, NAFTA should contain an explicit commitment that the Parties will not adopt or maintain any measure that restricts the cross-border transfer of data, including personal data. NAFTA should also prohibit the Parties from mandating that data centers or other computing facilities are located domestically, or requiring the use of domestic products or technologies. Any exceptions should be narrowly limited to ensure that they are necessary to achieve a legitimate public policy objective, and do not discriminate against foreign service providers in arbitrary ways. The agreement should also prohibit measures that require the transfer of technology, such as source code or algorithms, or the disclosure of trade secrets as a condition of market access.

In addition, the agreement should promote cooperation among NAFTA governments on cybersecurity matters; provide providers with protection against intermediary liability; encourage the use of innovative technology in government and modernize procurement rules; ensure that governments do not undermine encryption in commercial products; and prohibit customs duties on e-commerce or digital data.

---

<sup>16</sup> For BSA's full agenda on modern digital trade, see BSA, *Modernizing Digital Trade: An Agenda for Software in NAFTA and Beyond*, available at <http://www.bsa.org/~media/Files/Policy/Trade/05222017BSANAFTHandoutPress.PDF>.

A modernized NAFTA agreement with these key elements would stimulate significant economic growth and strengthen the United States' leadership on digital trade issues.

B. EU-U.S. Privacy Shield

The EU-U.S. Privacy Shield framework provides another important opportunity to promote digital trade. The Privacy Shield, which replaced the U.S.-EU Safe Harbor Framework, strengthens transatlantic trade by facilitating data transfers between the United States and the EU that are critical to digital services affecting a wide range of industries. Since its launch last year, over 2,500 companies have self-certified to participate in the Privacy Shield, including many BSA members.

The Privacy Shield contains several new obligations that participating companies must undertake to protect the privacy of personal data, and companies have taken substantial steps to comply with these new requirements, resulting in robust privacy protections. The United States government also has made several commitments to ensure the success of the framework, including those related to its general administration of the program and creation of procedures to address concerns that implicate national security issues.

The U.S. government and the European Commission agreed to conduct an annual review of the Privacy Shield to assess the progress of its implementation. The first annual review, which occurred last month, was an important opportunity for the Administration to highlight the significant work that it has undertaken to fulfill its commitments, including devoting increased resources to the administration of the program; ensuring sufficient remedies are available to EU citizens by implementing important aspects of the arbitration program; developing procedures

for the Ombudsman who handles complaints that implicate national security issues, and announcing the nomination of officials to key position posts, such as the Chairman of the Privacy and Civil Liberties Oversight Board.

We applaud the Administration's commitment to the Privacy Shield framework and the continued support from Congress to help amplify its importance to transatlantic digital trade.

C. Strengthening Relationships with Other Key Trade Partners

Finally, as other countries seek to stimulate economic growth by modernizing their trade policies, the United States should leverage these opportunities to ensure that it is engaging with key global partners, and to encourage our trading partners to continue to adhere to trade policies that facilitate data-driven economic activity and protect against market access barriers for e-commerce and digital trade. American technology companies and their customers are at the forefront of using data analytics, AI, and other data-driven tools to innovate, compete more effectively, and create new jobs. It is vital that, at this critical juncture, the United States does not cede its policy leadership on these issues to countries with agendas and interests that might conflict with our own.

\* \* \*

We appreciate Congress's leadership on the important issue of preserving the ability to transfer data across borders, which fuels job creation and economic growth. Thank you and I look forward to your questions.

Mr. LATTA. Well, thank you very much for your testimony.  
And, Mr. Garfield, you are recognized for 5 minutes. Thank you.

**STATEMENT OF DEAN C. GARFIELD**

Mr. GARFIELD. Thank you, Chairman Latta, Ranking Member Schakowsky, members of the committee. On behalf of 62 of the world's most dynamic and innovative companies, as well as my colleagues at ITI, I thank you for the opportunity to present at this hearing and for your efforts to spotlight this important issue.

This hearing arrives at an opportune time. We submitted my testimony for the record. So rather than repeat it, what I will do is highlight three things. One, why this issue is so important. Two, our sense of the state of play. And then, three, where we see gaps where your efforts in American leadership could be particularly valuable.

On the first, this issue is so important because, in many respects, digital trade and cross-border data flows are the air that sustains 21st century commerce. Moreover, the United States has a comparative advantage that will be unfairly undermined without vigilance and our intervention.

It is hard to think of anything that we do today that doesn't involve cross-border data flows in digital trade. Just my day today reflects that. When I got up this morning, I decided to go on a run and to download some music. Because the cloud servers that Ms. Espinel mentioned, and content-distribution networks are distributed all around the world, the music that I downloaded resulted in cross-border data flows. When I got in my car and drove here, and stopped at the grocery store, my car, the farming equipment for the food that I bought, as well as the delivery truck, have sensors to ensure safety that involve cross-border data flows and digital trade. I flew back from California yesterday. And while I was on my flight, my airplane has sensors that are making sure that the flight gets there safely, and if there is a problem when we get to the ground, that the ground crew is prepared to deal with any problems that may exist. Cross-border data flows, digital trade.

I could go on and on, but I think you get the point. While cross-border data flows and digital trade involve technology, it is not a technology issue. It is an all-of-America economic issue. In fact, America has a significant economic comparative advantage in digital trade and cross-border data flows. Ms. Espinel mentioned cloud servers. Seventeen of the top 20 cloud companies in the world are based here in the United States.

What is the state of play? Most countries around the world see that comparative advantage and are unwilling to sit by and watch it continue to exist. In China, for example, we face a tapestry of rules that are aimed at undermining that comparative advantage, whether it is forced localization or check and IP transfer, source code transfers, we see that catching fire. So markets like Indonesia and Vietnam are doing the same.

In other markets, including in some of our allies like Europe, we see some of the same. While the motivation may be quite distinct, the end result is the same, which is undermining the competitive advantage and comparative advantage of U.S. companies, and, from our perspective, doing damage to their own economy.

What can Congress do about it and what should it do? I endorse all of the things that Victoria mentioned, and would add two more. One is that Congress, in passing the bipartisan Trade Prioritization and Accountability Act, TPA, made the point that digital trade should be a point of emphasis. While we have a number of trade agreements that are progressing today, where the opportunity exists to advance digital trade, whether that is in NAFTA, which we strongly support and hope the administration will as well, or in the efforts around the KORUS Agreement, and upgrading that agreement as well, which we also view as incredibly important, the opportunity exists to make sure that we continue to advance our competitive advantage in American interests in a way that is fair.

The second is that acting in America's interests means, in this instance, working with the rest of the world. And so, second, we have an opportunity here to provide global leadership on what the rules of the road should be on digital trade and cross-border data flows. The President has announced that he is heading to China in November. That is an opportunity to work with the Chinese to bring them onboard to following global rules around digital trade.

We are hopeful that in working with Congress and working with the administration, we can ensure that this issue, which is so fundamental to America's leadership in the world, is prioritized but also acted on appropriately.

Thank you for the time.

[The prepared statement of Mr. Garfield follows:]

**Testimony of Dean Garfield  
President and CEO, Information Technology Industry Council (ITI)  
Hearing on Effects of Digital Trade on U.S. Businesses  
Before the Subcommittee on Digital Commerce and Consumer Protection  
Committee on Energy & Commerce**

**October 12, 2017**

Chairman Latta, Ranking Member Schakowsky, and Distinguished Members of the Subcommittee on Digital Commerce and Consumer Protection, thank you for the opportunity to appear before you today to discuss the critical importance of digital trade to U.S. innovation, competitiveness, job creation, and economic growth. As the Subcommittee with jurisdiction over non-tariff trade barriers, which most digital trade barriers are, we appreciate your leadership in engaging on these issues as the U.S. seeks to modernize the North American Free Trade Agreement and examines other trade agreements that were completed prior to the internet playing the role in the economy that it does today.

ITI is the global voice of the tech sector and we appreciate the opportunity to provide testimony on global digital trade. ITI members participate in and power digital trade across the globe. They manufacture hardware, develop software, create online content and platforms, provide services, and are key partners of companies of every size and across every industry that rely on digital technologies to further their business operations. Governments are also increasingly important customers for our members, as technology allows governments to reach more citizens with services and creates efficiencies within their operations. As the premier advocacy and policy organization for the world's leading innovation companies, ITI navigates the relationships between policymakers, companies, and non-governmental organizations, providing creative solutions that advance the development and use of technology around the world. ITI's testimony will focus on describing: 1) "digital trade," 2) its importance to the U.S. economy, 3) risks to digital trade, and 4) ideas for maximizing the benefits of digital trade to the U.S. economy, companies, and workers.

**What is “Digital Trade?”**

It is important to be clear about what we mean when we say “digital trade.” The U.S. International Trade Commission (ITC) defines “digital trade” as “U.S. domestic commerce and international trade in which the Internet and Internet-based technologies play a particularly significant role in ordering, producing, or delivering products and services.” In my view, the definition is both more basic and more expansive. Digital trade is simply any economic activity involving the movement of digital information (or “data”) across borders.

In other words, digital trade is exceptionally broad. Technology companies such as IBM, Microsoft, and Intel rely on cross-border data flows to address important objectives, such as improving public health, environmental stewardship, and connecting devices and people. It occurs when one purchases goods and services from an online retailer in another country, such as Uniqlo, a clothing company in Japan. It occurs when companies send digital information around the world to manage their businesses, such as Rio Tinto, the global mining company, which uses data to coordinate its global operations and relationships with its customers. It occurs when service providers sell their products electronically to overseas customers, such as when an insurance company underwrites life insurance policies for people in other countries. And it occurs when an individual in the European Union downloads smart phone applications developed in the United States. In other words, in 2017 digital trade happens all the time, every day, in a multitude of ways in all sectors of the economy and depends implicitly on the movement of digital information across borders.

**Why is Digital Trade Important to the U.S. Economy?**

The United States benefits greatly and disproportionately from digital trade. The ITC has estimated that U.S. GDP increased between \$517 billion and \$710 billion (3.4 to 4.8 percent) in 2011 as a result of digital trade, and that digital trade helped create 2.4 million jobs in the United States the same year.<sup>1</sup> The ITC also

---

<sup>1</sup> See U.S. International Trade Commission (ITC), *Digital Trade in the U.S. and Global Economies, Part 2*, (U.S. ITC,

found that, in 2012, small and medium-sized enterprises (SMEs) sold some \$227 billion in goods and services online. At the end of September, the ITC issued another report on global digital trade that revealed even more about the importance of digital trade to the United States:

- **Global digital trade is growing quickly as Internet usage is increasingly cloud-based.** Four U.S. companies (Amazon, Microsoft, Google, and IBM) are the top global providers of cloud computing services. The United States (\$44 billion), EU (\$15 billion), and China (\$1.3 billion) spent the most on public cloud computing services in 2015.
- **Global e-commerce grew from \$19.3 trillion in 2012 to \$27.7 trillion in 2016.** Business to Business (B2B) e-commerce makes up more than 86 percent of that total. Top Business to Consumer (B2C) e-commerce markets in 2015 were China (\$767 billion) and the United States (\$595 billion).
- **Internet usage is increasingly moving to the cloud.** Using industry data, the Commission estimates that 70 percent of all 2015 global Internet traffic went through cloud data centers—a striking increase from 2011, when only 30 percent went through those centers.
- **The United States is the largest market for cloud services** and home to some of the largest cloud service providers. U.S. firms such as Amazon Web Services, Google Cloud Platform, Microsoft Azure, and IBM Rackspace are the largest providers of cloud services for the global market, which had total estimated revenues of \$89.9 billion in 2016.
- **Global e-commerce grew from \$19.3 trillion in 2012 to \$27.7 trillion in 2016.** Business to Business (B2B) e-commerce makes up more than 86 percent of that total. Top Business to Consumer (B2C) e-commerce markets in 2015 were China (\$767 billion) and the United States (\$595 billion).

The most important message I would like to convey to you today is that the internet, digital technologies, and, therefore, digital trade, are fundamental to the competitiveness and success of U.S. companies in all

---

August 2014), <http://www.usitc.gov/publications/332/pub4485.pdf>.

sectors and of all sizes, to making international trade and the global economy more inclusive, and to making people's lives better. The international flow of data contributed \$2.8 trillion to the global economy in 2014, a figure that could reach \$11 trillion by 2025, according to McKinsey Global Institute. Digital trade is not just a tech sector issue, it's a whole of economy issue, and will only grow in significance as more companies use digital technologies to access markets, interface with customers, and innovate.

While the economic value generated by technology companies is incredibly significant (they employ over 6.9 million Americans — 5 percent of private sector employment — and account for 7.5 percent of U.S. GDP), digital trade often has its greatest impacts in business-to-business contexts, outside of the technology sector. Technology products and services that underpin digital trade drive growth and job creation in virtually every sector of the economy.

The U.S. Congress has recognized the importance of digital trade in many forms, most importantly when it enacted the Bipartisan Congressional Trade Priorities and Accountability Act of 2015 (“TPA”). As a whole, it was the first TPA bill that recognized the impact the internet has had on the U.S. economy and the significant competitive advantage for U.S. companies provided by minimizing barriers to the trade and export of digital goods and services. The 2015 TPA bill acknowledged the central importance of digital trade and cross-border data flows to the U.S. economy by recognizing them as “principal trade negotiating objectives.” In addition to protecting cross-border data flows, TPA gave specific direction to U.S. negotiators in several areas impacting digital trade, including modernized intellectual property and trade secrets protections, protections on requirements to transfer technology or source code, and the treatment of digital goods at the border.

Business owners across the U.S. economy — whether in the automotive, construction, energy, financial services, hospitality, manufacturing, retail, or other sectors — rely on cross-border data flows to run their businesses.

Let me give a few concrete examples of companies using our technologies and innovations in their business operations:

- **Caterpillar:** 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.<sup>2</sup>
- **AeroFarms:** New Jersey-based AeroFarms utilizes 95 percent less water than traditional farms by growing an array of lettuces and herbs in indoor vertical farms that can be located near highly populated cities such as Newark. The innovative company can also grow 100 times more kale, arugula, and watercress than your traditional farm that relies on sunlight and soil. With a pilot project in the Middle East under their belt and the support of 118 employees, the company is expanding domestically and is just beginning their global journey. AeroFarms is in the midst of developing vertical farms throughout the United States and across 4 continents with China and the United Arab Emirates as their areas of focus at the moment. The internet plays an integral part in facilitating AeroFarms' ability to deliver its innovative technology on a global basis. The vertical growing towers function more like data centers than farms. They are filled with sensors that capture data during every step in the planting process, which are used to perfect growth algorithms. AeroFarms' marketing team

---

<sup>2</sup> Information Technology and Innovation Foundation testimony at the House Ways and Means Trade Subcommittee Hearing on "Expanding U.S. Digital Trade and Eliminating Barriers to Digital Exports": <https://waysandmeans.house.gov/wp-content/uploads/2016/07/20160713TR-Atkinson-Testimony.pdf>

manages its company Facebook, Twitter, LinkedIn and YouTube presence, which easily attracts interest from the media and customers. Restaurateurs and chefs share on AeroFarms' website and Facebook page how they have converted to using "Dream Greens," the company's new retail brand of locally-grown, pesticide-free, non- GMO baby greens.<sup>3</sup>

- **Merck:** Merck has partnered with Numerate, a technology platform company leveraging proprietary algorithms alongside the power of cloud computing to transform the drug-design process, in order to generate novel small-molecule drug leads for an undisclosed cardiovascular disease target. Numerate's algorithms provide predictive models for molecular properties with accuracies comparable to laboratory testing, enabling scientists to search through billions of compounds to rapidly and efficiently identify those with the highest probability of activity against a specific target. This type of computational bioscience combines knowledge of the biocode with exploding empirical data to clear the way for scientists to design new therapies in the cloud. Such approaches could dramatically reduce the cost of pharmaceutical development and greatly expand the number of therapies that can be created and tested by moving medical research away from a "hit-and-hope" world of trial-and-error guesswork.<sup>4</sup>
- **The Interpublic Group of Companies:** Interpublic Group (IPG) is a global leader in modern marketing and advertising services, with more than 80 operating units and 47,000 employees in all major world markets. IPG is home to communications companies that provide consumer advertising, digital marketing, sports and entertainment marketing, public relations, and media services to many of the world's largest marketers. IPG Mediabrands, a division of the company, manages media strategy and placement services on behalf of clients, investing \$37 billion in global media in more than 120 countries. IPG Mediabrands relies on the free flow of data to identify advertising targets and media buys, develops the means by which to reach those targets, and evaluates the success of advertising

---

<sup>3</sup> Global Innovation Forum report on "The New Faces of American Trade"  
<http://globalinnovationforum.com/flipbook/inc/pdf/GIF-New-Faces-US-Trade-2017-web.pdf>

<sup>4</sup> Information Technology and Innovation Foundation report on "How Cloud Computing Enables Modern Manufacturing": <http://www2.itif.org/2017-cloud-computing-enables-manufacturing.pdf>

campaigns on behalf of its clients. IPG agencies work with clients around the world to evaluate and refine their global digital marketing and advertising campaigns by aggregating behavioral and demographic consumer information through regional processing centers. By collecting performance metrics like the number of ad views and clicks, as well as social media presence (e.g., Tweets, Facebook posts, blogs, Tumblr feeds, LinkedIn profiles), IPG agencies help their clients optimize and personalize the website advertisements shown to consumers across the world.<sup>5</sup>

In light of these examples, it is clear that U.S. companies and American workers have distinct competitive advantages in precisely the kinds of economic activities that digital trade facilitates:

- The United States is a leader in creating new industries, and Internet-related technologies are no exception. Seventeen of the top 20 enterprise cloud computing companies are headquartered in the United States,<sup>6</sup> as are seven of the top 10 Internet firms.<sup>7</sup>
- The United States excels in services, which are increasingly provided digitally. According to the Bureau of Economic Analysis (BEA)<sup>8</sup>, in 2014, exports of services that rely on information and communications technologies were \$385.1 billion, and imports of such services were \$230.9 billion, resulting in a trade surplus of \$154.2 billion. U.S. firms and American workers are disproportionately successful in selling services – such as research and development services, professional and management consulting services, architectural and engineering services, industrial engineering, and training services – to customers outside the United States.

<sup>5</sup> Business Roundtable report on “Putting Data to Work”:  
<http://businessroundtable.org/sites/default/files/reports/BRT%20PuttingDataToWork.pdf>

<sup>6</sup> See International Trade Administration (ITA), “2015 Top Market Report Cloud Computing” (ITA, July 2015),  
[http://trade.gov/topmarkets/pdf/Cloud\\_Computing\\_Top\\_Markets\\_Report.pdf](http://trade.gov/topmarkets/pdf/Cloud_Computing_Top_Markets_Report.pdf).

<sup>7</sup> See 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>.

<sup>8</sup> [https://www.bea.gov/scb/pdf/2016/05%20May/0516\\_trends\\_%20in\\_us\\_trade\\_in\\_ict\\_services2.pdf](https://www.bea.gov/scb/pdf/2016/05%20May/0516_trends_%20in_us_trade_in_ict_services2.pdf)

- The United States dominates in products and services involving high proportions of intellectual property. According to the U.S. Patent and Trademark Office (USPTO)<sup>9</sup>, total merchandise exports of IP-intensive industries increased to \$842 billion in 2014 from \$775 billion in 2010. Exports of service-providing IP-intensive industries totaled about \$81 billion in 2012 and accounted for approximately 12.3 percent of total U.S. private services exported in 2012.
- U.S. manufacturers tend to rely on globally integrated business networks to design, produce, and deliver their products. U.S. companies use digital technologies to optimize their operations and produce world-class products.
- U.S. small businesses are significant beneficiaries of digital trade. According to the Small Business Administration (SBA)<sup>10</sup>, U.S. small businesses employ almost half of the U.S. workforce and create two-thirds of all net new jobs. U.S. small businesses are thriving on the digital platforms created by technology companies. For example, according to a study by eBay<sup>11</sup>, the cost of trading on eBay's online marketplace fell by 41 percent between 2005 and 2009, three times faster than the decline in costs for traditional trade. Over 90 percent of eBay's U.S. businesses trade across borders. More than 80 percent of small businesses on eBay reach five or more markets. Amazon, for instance, now hosts some 2 million third-party sellers. In 2014, Facebook estimated that 50 million SMEs are on its platform, up from 25 million in 2013.<sup>12</sup>

In other words, digital trade is about much more than technology policy. It is about how business is done in the 21<sup>st</sup> century and, by extension, the opportunities that we in the United States have to enable innovation, enhance competitiveness, create jobs, and power economic growth. Simply put, digital trade plays to our strengths.

<sup>9</sup> <https://www.uspto.gov/sites/default/files/documents/IPandtheUSEconomySept2016.pdf>

<sup>10</sup> <https://www.sba.gov/sites/default/files/advocacy/Issue-Brief-11-Small-Biz-Key-Players-International-Trade.pdf>

<sup>11</sup> [https://www.ebaymainstreet.com/sites/default/files/EBAY\\_US-Marketplace\\_FINAL.pdf](https://www.ebaymainstreet.com/sites/default/files/EBAY_US-Marketplace_FINAL.pdf)

<sup>12</sup> <http://www.mckinsey.com/business-functions/digital-mckinsey/our-insights/digital-globalization-the-new-era-of-global-flows>

### **What are the Risks to Digital Trade?**

Just as opportunities for digital trade support U.S. competitiveness, job creation, and economic growth, barriers to digital trade threaten them. In recent years, governments around the world have adopted measures that interfere with the movement of data across borders, discriminate against U.S. firms, and, as a result, undermine U.S. economic interests. Such measures include: 1) restrictions on cross-border data flows; 2) requirements to localize data, production, or facilities; 3) mandates that companies transfer technology, such as source code, algorithms, or encryption keys; 4) stripping of “intermediary liability” protections, making online services liable for the conduct of third parties that they do not control; 5) the imposition of tariffs, taxes, and other charges on data flows or digital products; and 6) the extension of telecommunications and broadcasting regulatory requirements to online services.

Both ITI members and companies across the U.S. economy experience a wide-range of barriers to digital trade across the world that, taken together as a whole, make the internet less global and open, restrict cross-border data flows, and, therefore, reduce U.S. competitiveness.

A globally competitive technology sector that benefits the U.S. economy, businesses, and workers depends on preventing, reducing and eliminating these barriers, either through negotiation or enforcement of existing rules. The primary type of barrier to digital trade we have identified is the data localization requirement (see Exhibit A, a time series chart that demonstrates the steep rise in these requirements), for example in China, Indonesia, Nigeria, Russia, Turkey, and Vietnam. Our ITI Snapshot of Data Localization Requirements<sup>13</sup> (see Exhibit B) lists 18 data localization measures in force and six potential measures. The Information Technology and Innovation Foundation (ITIF) found data localization requirements in force in

---

<sup>13</sup> <https://www.itic.org/public-policy/SnapshotofDataLocalizationMeasures1-19-2017.pdf>

36 countries around the world.<sup>14</sup> The European Center for International Political Economy (ECIPE) has identified 22 data localization measures in force in European Union Member States and 35 restrictions on data usage that could indirectly localize data within EU Member States.<sup>15</sup> The economic impact of these measures is clear: data localization requirements increase costs for local companies by 30-to-60 percent according to a 2015 study by the Leviathan Security Group.<sup>16</sup> ECIPE estimates that these measures also detract from GDP growth, productivity, and competitiveness in the economies implementing them.<sup>17</sup>

The problem is not that governments are seeking to address the public policy issues raised by an increasingly digital world. Indeed, many of the stated motivations behind governments' policy choices are legitimate ones. It is appropriate, for example, for governments to work to ensure national security and public safety, support economic growth and job creation, and protect people's privacy and personal information. The problem is that, even when they have the right motivations, governments are too often pursuing the wrong policies. In other cases, governments are using legitimate motivations as smokescreens for protectionist efforts to advantage their own firms.

Consider the steps that China has taken in recent years to interfere with the activities of U.S. technology firms. For the purported reason of protecting its national security, China has in a few short years enacted a tapestry of laws, regulations, and unwritten rules that discriminate against foreign companies and effectively extract their intellectual property for national use. Chinese policies and practices violate virtually every "best practice" of digital trade. They restrict cross-border data flows, require the localization of data and facilities within the country, mandate the disclosure of source code and other proprietary knowledge as a condition of doing business, and otherwise put a thumb on the scale in favor of Chinese firms.

---

<sup>14</sup> [http://www2.itif.org/2017-cross-border-data-flows.pdf?\\_\\_ga=2.142742901.1791787411.1493816527-1581443156.1467220103](http://www2.itif.org/2017-cross-border-data-flows.pdf?__ga=2.142742901.1791787411.1493816527-1581443156.1467220103)

<sup>15</sup> <http://ecipe.org/app/uploads/2016/12/Unleashing-Internal-Data-Flows-in-the-EU.pdf>

<sup>16</sup> <http://www.leviathansecurity.com/blog/quantifying-the-cost-of-forced-localization>

<sup>17</sup> [http://www.ecipe.org/app/uploads/2014/12/OCC32014\\_\\_1.pdf](http://www.ecipe.org/app/uploads/2014/12/OCC32014__1.pdf)

Or take the example of the many developing countries that are restricting data flows and requiring localization measures in hopes that this will stimulate their domestic economic development:

- A number of Indonesian measures, including its “Information and Electronic Transaction Law” and “Government Regulation 82,” require that any company providing internet-enabled services to locate its data centers domestically.
- Nigeria’s “Guidelines for Nigerian Content Development in ICT” require that all consumer and subscriber data collected by companies in Nigeria be hosted within Nigeria.
- Vietnam’s Decree on Information Technology Services mandates that companies that provide internet-enabled services maintain at least one server within the country.

With such measures, governments not only work against their own economic policy interests by depriving their firms, workers, and consumers of cutting-edge technologies, products, and opportunities, they also effectively prevent American companies and small businesses from selling their products and services to hundreds of millions of people overseas.

A final example concerns the recent efforts of the European Union (EU) and the United States to agree on a mechanism for transatlantic data transfers. Like the United States, the EU has an admirably high level of legal protection for personal data, and it understandably wants to ensure that EU citizen data is appropriately protected when it is sent to third countries. Also like the United States, EU companies and citizens benefit greatly from the economic opportunities that cross-border data flows provide. Yet instead of agreeing to international rules guaranteeing cross-border data flows – subject to thoughtful, targeted exceptions to protect personal information – the EU seeks a blanket exemption of its data protection laws from any trade rules. It also maintains dozens of poorly justified data localization measures across its Member States. The effect of the EU’s policies and practices on data is to create great uncertainty on the part of companies,

many of which are based in the United States, regarding whether it will be legal or practical to move data across the Atlantic.

**What can we do to Maximize the Benefits of Digital Trade to the United States?**

We are at an inflection point in our policy choices about digital trade. Given the rapid pace of technological innovation, governments around the world are having to make choices about the regulatory structures that they want for the movement of digital information across borders. In our view, as discussed above, many governments are making the wrong choices. Whether for valid reasons or as pretexts for protectionism, many economies are imposing barriers to the movement of data and related economic activity that not only harm their own growth and development prospects, but also undermine the competitiveness of U.S. companies and the living standards of American citizens.

The United States has an opportunity to show global leadership in crafting policy environments that support cross-border data flows, open markets, and enhance economic opportunity at home and around the world. Congress has a critical role to play in effectuating this leadership, not only because of its constitutional authority over international trade but also because it has done so before. The general policy recipe that Congress has articulated in recent years is the right one, and both Members of Congress and their staffs are well-positioned to provide the kinds of oversight and support that a well-designed U.S. policy on digital trade demands.

**Conclusion**

In that regard, it is worth recalling the three broad priorities that we identified for the Administration earlier this year, priorities that we would welcome Congress' support in pursuing.<sup>18</sup>

---

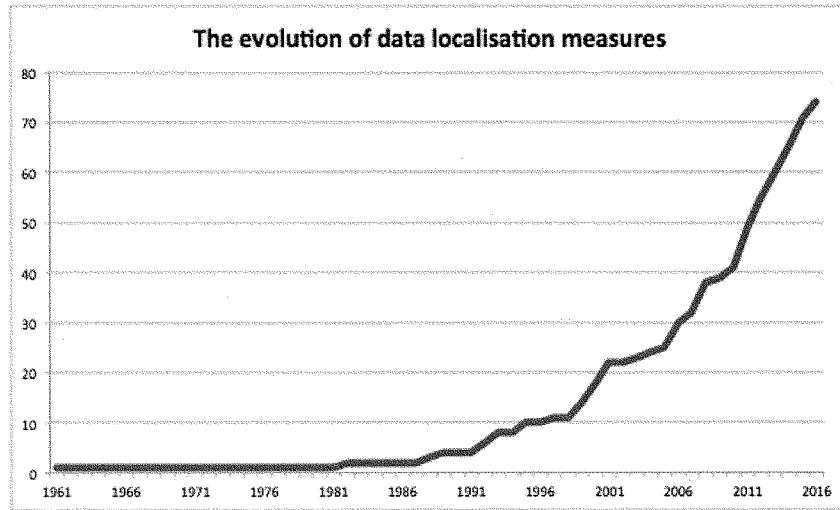
<sup>18</sup> <https://www.itic.org/news-events/news-releases/iti-outlines-tech-sector-s-trade-priorities-to-us-trade-representative-lighthizer>

- **New Rules.** A globally competitive technology sector that benefits the U.S. economy, businesses, and workers depends not only on the enforcement of existing trade rules, but also on the negotiation of new rules that reflect the fundamentally digital nature of our economy and that prevent or eliminate barriers to digital trade. Ideally, as the United States government and other governments address barriers to digital trade, whether through trade agreements or other policy mechanisms, they would work to establish new international norms that ensure that the internet remains free, open, and global, including allowing data to flow freely across borders; prohibiting tariffs or other taxes on cross-border data flows and digital products; prohibiting discrimination against new services that innovative companies using digital technologies provide; prohibiting requirements to localize data, production, or infrastructure; prohibiting forced transfers of technology, source code, algorithms, or encryption; and ensuring the adoption of strong intermediary liability protections.
- **Enforcement.** It is also critical that the U.S. government enforce U.S. trade agreements to ensure our companies and workers can compete fairly. The rules in our trade agreements should ensure that U.S. companies and workers are treated fairly and have an equal chance to compete in markets around the world. Enforcement of these rules is critical to U.S. industry. We, therefore, encourage an active and aggressive approach to enforcement of U.S. trade agreements, targeted at problems of significant concern.
- **Resources.** To advance successful negotiating and enforcement agendas, we advocate that the U.S. government increase its efforts and resources to support a digital agenda in U.S. trade policy. Specifically, we recommend that USTR elevate and increase its digital trade efforts by designating a senior official responsible for digital trade and adding resources at all levels of the agency. These steps would be commensurate with the large and growing impact of digital technologies on the global economy and U.S. competitiveness. Last year, the Departments of State and Commerce enhanced their support for the digital economy with their digital attaché programs; we have encouraged expansion of these programs to more markets. These agencies also have specific responsibilities, including in administering the EU-U.S. Privacy Shield. USTR also took a complementary and

important step of creating an internal working group on digital issues. More focus is needed, however, especially in light of the TPA negotiating objectives on digital issues; increasing evidence that technology can make trade more inclusive; and the growing barriers impeding trade in digital technologies. Given this Subcommittee's role in authorizing the Commerce Department's activities and budget, additional oversight in this area would be greatly appreciated.

\* \* \*

## EXHIBIT A



## EXHIBIT B

## Data Localization Snapshot

Current as of January 19, 2017

Active Measures		
Country	Measure	Details
Australia	<u>Personally Controlled Electronic Health Record Provision</u>	This regulation restricts the exportation of any personally identifiable health information.
Canada	Two provincial personal information laws: <u>Nova Scotia</u> and <u>British Columbia</u>	These two provincial laws restrict the exportation of any personal data collected by or for public bodies.
China	<u>Cyber-Security Law</u>	This law contains broad requirements for local processing and storage of "important data" related to Chinese citizens and critical information infrastructure.
China	<u>Notice to Urge Banking Financial Institutions to Protect Personal Information</u>	This law prohibits the off-shore analyzing, processing, or storage of Chinese personal financial information.
China	<u>Guidelines for Personal Information Protection within Public and Commercial Information Systems</u>	This standard prohibits the overseas transfer of data without express user consent or government permission.
China	<u>Online Publishing Service Management Rules</u>	This law requires that all servers used for online publishing in China be located within China.
China	<u>Population and Healthcare Information Management Measures</u>	These measures prohibit the overseas transfer of health and medical information.
Germany	<u>Telecommunications Act</u>	Amendments to this act require telecommunications providers to store meta data for a specified period of time within the borders of Germany.
India	<u>National Data Sharing and Accessibility Policy</u>	This policy requires all data collected using public funds to be stored within the borders of India.
Indonesia	<u>Regulation No. 82: Information and Electronic Transaction Law</u>	This law mandates that any company which provides internet enabled services directly to the consumer must locate their data centers within Indonesia.
Kazakhstan	<u>Amendments to Certain Legislative Acts on Informatization</u>	These amendments require that all personal data collected within Kazakhstan be stored within the country.
Korea	<u>Act on the Establishment and Management of Spatial information</u>	This act, an update to a law which originated in the Korean War era, greatly restricts the cross-border transfer of mapping data.
Nigeria	<u>Guidelines for Nigerian Content Development in ICT</u>	These guidelines require that all consumer and subscriber data collected by companies in Nigeria be hosted within Nigeria.
Russia	<u>Federal Law 242-FZ</u>	This law requires that all data collected on Russia citizens be stored within Russia.

Russia	<a href="#">Federal Law 149-FZ</a>	This law: 1) Requires any organization which “disseminates” information on the internet (email, messaging services, etc.) must keep all metadata within Russia for 6 months; and 2) all bloggers with more than 3,000 followers must register with local authorities.
Turkey	<a href="#">E-Payment Law</a>	This law requires companies that provide e-payment services to conduct all data processing within the borders of Turkey.
United States	<a href="#">DoD Interim Rule on Network Penetration Reporting and Contracting for Cloud Services</a>	These rules require that all cloud computing service providers that work for the DOD to store DOD data within U.S. Territory.
Vietnam	<a href="#">Decree of Information Technology Services</a>	This law mandates that all companies that provide a range of different internet enabled services maintain at least one server within the borders of Vietnam.
Potential Measures		
Country	Measure	Details
China	Draft Supervision Rules on Insurance Institutions Adopting Digitized Operations	This law would require localization of data servers by any insurance institution processing the personal data of Chinese citizens. Additionally, there are vague requirements for data residency that are yet to be defined.
China	Secure and controllable standards	In addition to highly invasive IP disclosure requirements, the regulation also has a section that gives preferred status to companies that can have upfront design duplicated environment of CPUs located within China.
Indonesia	Draft Regulation Regarding the Provision of Application and/or Content Services Through the Internet	This law has a vague requirement that OTT service providers place part of their data centers within Indonesia.
Korea	Standards for Cloud Computing Services	These pre-announced standards would require all cloud computing providers place servers handling public data within the borders of Korea.
Saudi Arabia	<a href="#">Proposed Regulation for Cloud Computing</a>	This proposed regulation would require cloud service providers to store certain types of data locally based on a four tier data classification system.
Vietnam	Draft OTT Circular	This draft law would require all OTT service providers to locate at least one server in Vietnam.

Mr. LATTA. Thank you very much for your testimony.

And, Ms. Daskal, you are recognized for 5 minutes. Thanks again.

#### **STATEMENT OF JENNIFER DASKAL**

Ms. DASKAL. Thank you. Chairman, ranking member, and members of the committee, thank you for inviting me to testify here today.

The free movement of data, as we have heard, is critical to economic growth, has benefits for data security, and promotes privacy, speech, and associational rights. Yet increasingly, states are adopting a range of measures that restrict data flows to the United States and elsewhere and adopting costly data localization requirements pursuant to which companies must store data locally.

Many of these restrictions are directed specifically at the United States or adopted in direct response to concerns about U.S. policies and market power. The motivating factors are multiple, including fears about the scope of U.S.-foreign intelligence surveillance, concerns about the adequacy of U.S. consumer privacy protections, a desire by foreign governments to ensure access to data that they seek for law enforcement investigations, and sheer protectionism.

There is, as a result, no single, all-encompassing solution. But there are also, nonetheless, important steps that the United States can and should take to address some of these motivating factors and promote a free and open internet. Specifically, I identify four key areas for reform.

First, improvements to key foreign intelligence surveillance rules so as to better promote both privacy and the free flow of data, while also continuing to protect national security. Second, the adoption of enhanced consumer privacy protections. Third, reforms to U.S. law to better facilitate law enforcement access to data across border, consistent with baseline substantive and procedural protections. And, fourth, the use of trade policy has been discussed already to preclude data localization mandates and impose penalties on those who engage in digital protectionism.

In my written testimony, I go into detail in all of these areas. But given my limited time here, I am going to focus on two: surveillance policy and law enforcement access to data across border.

As we have already heard, in 2015, the European Court of Justice sent shockwaves to the business community by striking down the then-in-place Safe Harbor Framework given, primarily, concerns about U.S. foreign intelligence surveillance. The Framework had been relied on by close to 5,000 companies to support the transfer of data from the EU to the United States.

The Safe Harbor Framework, as we have also heard, has now been replaced by Privacy Shield, which just underwent its first review. But both Privacy Shield, and an alternative basis for allowing such transfers of data from the EU, what is known as standard contractual clauses, are now subject to legal challenge. And, in fact, just 2 weeks ago, the Irish High Court referred one of those challenges back up to the European Court of Justice based on “well-founded” concerns about the scope of U.S. surveillance and accountability mechanisms. If these bases for transferring data from the

EU to the United States are struck down, it would be devastating to the free flow of data and to United States' businesses.

There are, however, reforms that Congress can and should push that would help respond to these concerns. In fact, the House Judiciary Committee's USA Liberty Act, introduced earlier this week, includes several such important reforms. Importantly, it codifies an already implemented restriction on so-called about communications pursuant to which communications that are about a foreign target and not just to or from the foreign target can be acquired. This kind of about collection yields large quantities of incidental collection on those that wouldn't be otherwise legitimate targets and is, thus, a source of concern.

The bill also sets up new transparency and accountability mechanisms, and, importantly, it includes improvements to the Privacy and Civil Liberties Oversight Board, which would allow it to better function. This board plays an important role in overseeing surveillance, policies, and, importantly, from a European perspective, reviewing complaints made by EU citizens regarding U.S. national security surveillance. It is now down to one member, so it can't currently function. So Congress also should push the administration to move forward the other four nominees needed to fill this board.

Secondly, Congress should also respond to the legitimate concerns of foreign law enforcement officers that find themselves subject to lengthy delays in accessing emails and other communication content of their own nationals in the investigation of local crime based simply on the fact that some of the data is U.S. held. Notably, the Obama administration, and again the Trump administration, have sent up legislation to Congress that would ease some of those restrictions and facilitate access to cross-border data for law enforcement investigations, subject to important baseline substantive and procedural protections. This is something that should be supported.

Collectively, these reforms are important to help ensure the free flow of data, to promote the U.S. in the global economy, and to protect data security and data privacy.

Thank you.

[The prepared statement of Ms. Daskal follows:]



AMERICAN UNIVERSITY  
WASHINGTON, D.C.

---

**Statement of  
Jennifer Daskal**

**Associate Professor  
American University Washington College of Law**

**Committee on Energy and Commerce  
Subcommittee on Digital Commerce and Consumer  
Protection  
United States House of Representatives**

**Hearing on  
*21st Century Trade Barriers: Protectionist Cross Border Data  
Flow Policies Impact on U.S. Jobs***

**October 12, 2017**

Statement of  
Jennifer Daskal  
Associate Professor  
American University Washington College of Law

Committee on Energy and Commerce  
Subcommittee on Digital Commerce and Consumer Protection  
United States House of Representatives

Hearing on  
21st Century Trade Barriers: Protectionist Cross Border Data Flow Policies Impact  
on U.S. Jobs

October 12, 2017

Chairman Latta, Ranking Member Schakowsky, and Members of the Committee, thank you for inviting me to testify.

The free movement of data across borders is critical to economic growth, has benefits for data security, and promotes privacy, speech, and associational rights. Yet, increasingly states are adopting a range of measures that restrict data flows to the United States and elsewhere and adopting costly data localization mandates, pursuant to which companies must store data locally.<sup>1</sup> Such restrictions on the free movement of data harm U.S. business interests, undermine the growth potential of the Internet and thus the global economy, and undercut both data security and privacy.

International data flows increased world GDP by 10 percent compared to a world without such flows, according to a recent McKinsey report.<sup>2</sup> The benefits for the United States are particularly strong. The U.S. International Trade Commission reports that digital trade—loosely defined as economic activity involving Internet technology and the cross-border movement of data—increased U.S. GDP by 3.4-4.8 percent in 2011, resulting in a significant increase in wages.<sup>3</sup> Restrictions on the free flow of data threaten this important source of economic growth.

Data security is also put at risk when service providers are forced to store all data on local servers, rather than distribute the data across different storage sites in multiple

<sup>1</sup> See, e.g., Anupam Chander & Uyen P. Le, *Data Nationalism*, 64 EMORY L. J. 677 (2015) (detailing a range of localization mandates); ALBRIGHT STONEBRIDGE GROUP, DATA LOCALIZATION: A CHALLENGE TO GLOBAL COMMERCE AND THE FREE FLOW OF INFORMATION (Sept. 2015), <http://www.albrightstonebridge.com/files/ASG%20Data%20Localization%20Report%20-%20September%202015.pdf>.

<sup>2</sup> SUSAN LUND, JACQUES BUGHIN, JONATHAN WOETZEL, KALIN STAMENOV, & DAN VADENBERG, DON'T STOP DATA FROM FLOWING: A CALL FOR A GLOBAL CHARTER ON DATA FREEDOM (McKinsey Global Institute, Dec. 2016), <http://www.mckinsey.com/business-solutions/digital/privacy-and-data-protection/globalization-the-new-era-of-global-flows>.

<sup>3</sup> U.S. INT'L TRADE COMMISSION, DIGITAL TRADE IN THE U.S. AND GLOBAL ECONOMIES, Part 2 13 (Aug. 2014), <https://www.usitc.gov/publications/332/pub4485.pdf>.

locations.<sup>4</sup> Localization mandates also can result in business being shifted from major online providers to smaller local equivalents. This too can create additional security risks. Smaller, local providers often have weaker security protections than major multinational companies with the resources to respond to increasingly sophisticated cyber thieves.<sup>5</sup>

Moreover, whereas data localization mandates are often described as a means of protecting privacy, they often have the converse effect. They provide a means for repressive regimes to keep tabs on citizens and residents in ways that can stifle dissent—or worse.

Such restrictions on the free flow of data are often directed specifically at the United States or adopted in direct response to concerns about U.S. policies and market power. The motivating factors are multiple—including fears about the scope of U.S. foreign intelligence surveillance, concerns about the adequacy of U.S. consumer privacy protections, a desire by foreign governments to ensure their own ability to access sought-after data, and sheer protectionism. There is, as a result, no single, all-encompassing solution. But there are nonetheless important steps that the United States can take to address some of the motivating forces and thereby promote a free and open Internet.

In what follows, I suggest four areas of reform designed to address each of the key concerns motivating such restrictions.

### 1. Surveillance Reform

Concerns about the reach of U.S. foreign intelligence surveillance have led foreign governments and foreign-based customers to seek out non-U.S.-based companies to manage their data and to insist on data localization—with significant costs to the U.S. tech industry.<sup>6</sup> In 2015, the European Court of Justice (ECJ) sent shock waves through the business community in the United States and Europe by striking down the then-in-place Safe Harbor Framework, largely due to concerns about U.S. intelligence surveillance in the wake of the Snowden revelations.<sup>7</sup> The Safe Harbor Framework had been relied on by well over 4,000 companies as a means of assuring (via a self-certification process) that they had “adequate” privacy protections in place as required by EU law, and thereby permitting the transfer of personal data from the EU to the United States.

<sup>4</sup> See DANIEL CASTRO, THE FALSE PROMISE OF DATA NATIONALISM 1 (Info. Tech. & Innovation Found., Dec. 2013), <http://www2.itif.org/2013-false-promise-data-nationalism.pdf> (“The notion that data must be stored domestically to ensure that it remains secure and private is false”).

<sup>5</sup> See Chander & Le, *supra* note 1, at 719.

<sup>6</sup> See, e.g., Claire Cain Miller, *Revelations of N.S.A. Spying Cost U.S. Tech Companies*, N.Y. TIMES, Mar. 21, 2014; DANIEL CASTRO & ALAN MCMCQUINN, BEYOND THE USA FREEDOM ACT: HOW U.S. SURVEILLANCE STILL SUBVERTS U.S. COMPETITIVENESS (Info. Tech. & Innovation Found., June 2015) [https://www.scribd.com/embeds/268099469/content?start\\_page=1&view\\_mode=scroll&show\\_recommendations=true](https://www.scribd.com/embeds/268099469/content?start_page=1&view_mode=scroll&show_recommendations=true) (asserting that concerns over U.S. surveillance practices in wake of the Snowden revelation are likely to cost the U.S. tech sector more than \$35 billion).

<sup>7</sup> See Case C-362/14, Maximilian Schrems v. Data Prot. Comm'r, 2015 E.C.R., ¶ 94-95, <http://curia.europa.eu/juris/document/document.jsf?docid=169195&doclang=EN>.

The subsequently negotiated Privacy Shield Framework is currently relied on by approximately 2,500 companies as a basis for engaging in the cross-continental transfer of personal data.<sup>8</sup> A range of companies also rely on what are known as standard contractual clauses, which offer an alternative means of establishing the legality of such transfers.<sup>9</sup> But both Privacy Shield and standard contractual clauses are subject to legal challenge as well—based on ongoing concerns about the reach of U.S. surveillance.<sup>10</sup> In fact, just two weeks ago, the Irish High Court concluded that there are “well founded concerns” about the adequacy of the privacy protections provided for by standard contractual clauses. The Irish Court focused on the reach of U.S. foreign intelligence surveillance and the perceived absence of effective remedies.<sup>11</sup> The case has now been referred to the ECJ.<sup>12</sup>

Meanwhile, several Members of the European Parliament also have expressed concerns about both the scope of U.S. surveillance and the absence of sufficient accountability mechanisms for EU citizens.<sup>13</sup> An expert group of European privacy officials have raised concern about bulk surveillance by the United States and the failure to staff the Privacy and Civil Liberties Board (PCLOB), which provides important oversight of U.S. surveillance policies and practices.<sup>14</sup> An ECJ ruling or broader policy determination that U.S. legal protections are inadequate to support cross-continental transfers of personal data would be devastating to the free flow of data from the EU to the U.S. and to U.S. businesses.

Some of the EU’s critiques reflect a mischaracterization of U.S. policies and practices and elide key changes to US surveillance policies and practices over the past several years. These include the passage of the Judicial Redress Act, which extends protections of the Privacy Act of 1974 to the citizens of the EU and other designated foreign countries;<sup>15</sup> the passage of USA Freedom Act, which put an end to the government’s bulk collection of domestic telephony metadata, requires declassification reviews of significant Foreign Intelligence Surveillance Court (FISC) opinions, and

<sup>8</sup> See Sam Schechner, *Europe’s Top Court to Review Privacy*, WALL ST. J. (Oct. 4, 2017).

<sup>9</sup> Other possible mechanisms for supporting the cross-continental transfer of personal data include consent by the data subject (although the standard for finding valid consent can be hard to meet); binding corporate rules (although these only permit intra-corporation transfers and do not allow transfers to unaffiliated entities, such as customers and suppliers); and reliance on approved codes or conduct. See Lothar Determan, Brian Hengesbaugh & Michaela Weigl, *The E.U.-U.S. Privacy Shield Versus Other EU Data Transfer Compliance Options*, BLOOMBERG BNA (Sept. 12, 2016) (detailing various transfer options).

<sup>10</sup> See Case T-670/16, *Dig. Rights Ireland v. Comm’n*, 2016 O.J. (C 410) 26; *Data Prot. Comm’r v. Facebook Ireland Ltd. & Maximilian Schrems (Schrems II)*, [2017] 2016 No. 4809 P (H. Ct) (Ir.) (Oct. 3, 2017), [https://iapp.org/media/pdf/resource\\_center/IrishHC-Fb-Schrems-decision-10-17.pdf](https://iapp.org/media/pdf/resource_center/IrishHC-Fb-Schrems-decision-10-17.pdf) (referring case to ECJ).

<sup>11</sup> *Schrems II*, [2017] 2016 No. 4809 P at ¶ 334.

<sup>12</sup> *Id.*

<sup>13</sup> See European Parliament resolution of 6 April 2017 on the adequacy of the protection afforded by the EU-US Privacy Shield, (2016/3018(RSP)), <http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//NONSGML+TA+P8-TA-2017-0131+0+DOC+PDF+V0//EN>.

<sup>14</sup> See Article 29 Data Protection Working Party, Press Release, *Preparation of the Privacy Shield annual Joint Review* (13 June 2017).

<sup>15</sup> Judicial Redress Act of 2015, Pub. Law No. 114-126 (2016).

mandates enhanced transparency about Foreign Intelligence Surveillance Act (FISA) collection;<sup>16</sup> and adoption of new executive branch guidance designed to better protect the privacy interests of foreigners.<sup>17</sup>

But ongoing concerns about the perceived overreach of U.S. foreign intelligence collection and the sufficiency of accountability mechanisms loom large, and there is more that Congress can do to assure the EU and other key allies that their concerns are being taken into account. Specifically, Congress can and should push for the following key reforms. Together, they will help assure foreign governments that the United States adequately protects the privacy interests of their citizens and residents and thereby better protect the free flow of data from the EU and elsewhere.

*First*, with section 702 of the Foreign Intelligence Surveillance Act of 2008 set to sunset this December, Congress should take this opportunity to implement additional protections designed to better safeguard privacy, consistent with the government's intelligence needs.<sup>18</sup> Among other reforms, Congress should codify the end to the collection of “about” communications—something the executive branch has already put a stop to as a matter of policy.<sup>19</sup> As the terminology suggests, an “about” communication contains a reference to (is “about”) an email or phone number associated with a particular target, rather than being directly to or from the target's email or phone number. It thus sweeps in a significant amount of incidental collection on those that would not otherwise be deemed legitimate, direct targets of such collection.

Notably, the House Judiciary Committee's recently released USA Liberty Act includes an eight-year prohibition on “about” collection; this is something that should be widely supported.<sup>20</sup> Other provisions of the USA Liberty Act require enhanced reporting and accountability measures, mandate the appointment of amicus curiae to the FISC to assist in the issuance of 702 certifications, and put in place improvements to the Privacy and Civil Liberties Oversight Board (discussed in more detail below); these too deserve wide support.<sup>21</sup> Such reforms would help to ensure the EU and other foreign governments that U.S. surveillance programs are subject to enhanced accountability

<sup>16</sup> USA FREEDOM Act of 2015, Pub. Law No. 114-23 (2015).

<sup>17</sup> See WHITE HOUSE, PRESIDENTIAL POLICY DIRECTIVE—SIGNALS INTELLIGENCE ACTIVITIES § 4 (Jan. 17, 2014), <https://obamawhitehouse.archives.gov/the-press-office/2014/01/17/presidential-policy-directive-signals-intelligence-activities> [hereinafter PPD-28].

<sup>18</sup> The 702 program authorizes the National Security Agency to, pursuant to Foreign Intelligence Surveillance Court approval of minimization and targeting procedures, acquire the communications of foreigners located outside the United States for the purposes of gathering foreign intelligence information. For a detailed analysis of the program. For an excellent overview of the 702 program, see PRIVACY & C.L. OVERSIGHT BD., REPORT ON THE SURVEILLANCE PROGRAM OPERATED PURSUANT TO SECTION 702 OF THE FOREIGN INTELLIGENCE SURVEILLANCE ACT (July 2, 2014), <http://www.pclob.gov/library/702-Report.pdf>.

<sup>19</sup> See Charlie Savage, *N.S.A. Halts Collection of Americans' Emails About Foreign Targets*, N.Y. TIMES (April 28, 2017).

<sup>20</sup> H.R. 3989, 115<sup>th</sup> Cong. § 102(a)(2) (2017).

<sup>21</sup> Additional reforms, some of which are also included in the USA Liberty Act, are also needed to protect the Fourth Amendment interests of U.S. persons, including limits on FBI searches of the databases for U.S. person information. Here, however, I am focused on reforms that would provide protections for U.S. persons and foreigners alike, consistent with the goal of promoting the free flow of data.

mechanisms and thus help preserve the free flow of data.<sup>22</sup>

*Second*, Congress should mandate what Presidential Policy Directive 28 (PPD-28) does as a matter of policy. PPD-28 was issued by President Obama in response, in large part, to foreign government concern about the scope of US surveillance and applies to all signals intelligence activity (not just that covered by 702). Specifically, Congress should codify the requirement that “signals intelligence activities . . . include appropriate safeguards for the personal information of all individuals, regardless of the nationality of the individual to whom the information pertains or where that individual resides.” Congress should also codify the presumption (taken from PPD-28) that protections for personal information collected through signals intelligence apply to U.S. citizen and foreign data alike: “To the maximum extent feasible consistent with the national security, these policies and procedures [designed to safeguard personal information] are to be applied equally to the personal information of all persons, regardless of nationality.”<sup>23</sup>

*Third* Congress should work with the administration to reinvigorate and put in place improvements to the Privacy and Civil Liberties Oversight Board (PCLOB). Created in 2007 and first operational in May 2013, the PCLOB provides oversight over foreign intelligence collection so as to ensure that such actions are balanced with the need to protect privacy and civil liberties. The PCLOB’s reports on both the telephony metadata program and the 702 collection programs have been highly influential—providing some of the most extensive information about these programs and ultimately contributing to the dismantling of the bulk collection of telephony metadata.<sup>24</sup> Of particular importance, the PCLOB has been designated as the review body for complaints referred by the Privacy Shield ombudsman, a position set up in the wake of Privacy Shield to receive and review complaints regarding national security access to data transferred from the EU to the US

Now down to one board member, the PCLOB lacks a sufficient quorum (three out of the five members) to continue to function. In an encouraging sign, the administration has recently nominated a new PCLOB Chair. Congress should move quickly to hold hearings on the nomination, push for the nominations of other board members, and reinvigorate this critically important oversight body. The PCLOB’s continued operation is something that can help ensure the continued vitality of Privacy Shield.

In addition, Congress should adopt the provisions included in the bipartisan USA Liberty Act that ensure the board can carry out key functions even during a period of vacancy by the Chair and permit board members to engage in informal discussions without being subject to the requirements of the Sunshine Act. Meanwhile, the

<sup>22</sup> H.R. 3989, *supra* note 20 §§ 103, 104, 107, 201-203.

<sup>23</sup> PPD-28, *supra* note 17, at § 5.

<sup>24</sup> See REPORT ON THE SURVEILLANCE PROGRAM OPERATED PURSUANT TO SECTION 702 OF THE FOREIGN INTELLIGENCE SURVEILLANCE ACT, *supra* note 18; REPORT ON THE TELEPHONE RECORDS PROGRAM CONDUCTED UNDER SECTION 215 (Jan. 23, 2014), [https://www.pclob.gov/library/215-report\\_on\\_the\\_telephone\\_records\\_program.pdf](https://www.pclob.gov/library/215-report_on_the_telephone_records_program.pdf).

provisions requiring that the Board hold public hearings, inform the public of its activities, make its reports public to the greatest extent possible should be kept intact.<sup>25</sup>

## 2. Consumer Privacy Protection

This summer's breach at Experian—pursuant to which the personal and confidential information of nearly half of the American's population was exposed—highlights once again the need for better consumer privacy protections in U.S. law. Enhanced consumer privacy requirements are things that any company doing business in Europe will already be familiar with—given the requirements of EU's soon to be implemented General Data Protection Regulation (GDPR). The GDPR, which will go into effect in May 2018, applies to all companies that process the personal data of EU data subjects, regardless of the company's location and mandates an array of protections for consumer privacy.<sup>26</sup> Enhanced consumer privacy protections will also help ensure the future of Privacy Shield—protecting it from legal and policy-related challenges.

In other words, strengthening consumer privacy protections is not only good policy, but something that just about any company that wants to do business in the EU is going to have to implement anyway, will help ensure the future of Privacy Shield, and will help to disincentivize protectionist policies based on a claimed need to protect consumer privacy.

I suggest three key reforms.

*First*, Congress should pass a strong data breach notification statute. This should set a minimal floor, putting in place strict obligations for timely and rolling notification, while also permitting states to innovate and demand more.<sup>27</sup> Pursuant to the GDPR, timely notification is something that companies doing business in Europe will already be required to do; breach notification to authorities is generally required within 72 hours, and notification to affected data subjects “without undue delay” in specified circumstances.<sup>28</sup> The fact that Equifax took some six weeks and perhaps longer to notify its customers about the breach should remind Congress of the need for legislative action in this area.

*Second*, Congress should enact a Privacy Act for the private sector—what has often been called a Consumer Bill of Rights.<sup>29</sup> Whereas the Privacy Act grants

<sup>25</sup> See 42 U.S.C. 2000ee(f); ADAM KLEIN, MICHELE FLOURNOY, AND RICHARD FONTAINE, SURVEILLANCE POLICY: A PRAGMATIC AGENDA FOR 2017 AND BEYOND 39 (Dec. 2017) (recommending that PCLOB be exempted from the Sunshine Act), <https://www.cnas.org/publications/reports/surveillance-policy>.

<sup>26</sup> Regulation (EU) 2016/679 of 27 April, 2016, General Data Protection Regulation, 2016 O.J. (L 119) [hereinafter GDPR].

<sup>27</sup> See, e.g., Danielle Citron, *The Privacy Policymaking of State Attorney General*, 92 NOTRE DAME L. REV. 747, 767-769 (2016) (describing data breach notification requirements being mandated by states).

<sup>28</sup> GDPR, *supra* note 26, arts 32-34.

<sup>29</sup> See *Examining the EU Safe Harbor Decision and Impacts for Transatlantic Data Flows: J. Hearing Before the U.S. H.R. Energy & Commerce Subcomms. on Commerce, Mfg., and Trade and Comm'ns and*

individuals a tool to learn about it and correct mistakes with respect to personal data in the hands of the federal government, there are no equivalent protections vis-à-vis the private sector. Congress should rectify this. It should ensure that individual consumers are provided a statutory basis to protect their own personal data and correct mistakes made and potentially promulgated by the private sector. And it should oblige the private sector to take reasonable steps to protect data security, coupled with the creation a private right of action.

*Third*, the Federal Trade Commission (FTC) should be given the authority to impose financial penalties for privacy and security violations, even the first time there is a compliance problem, and to impose larger fines than is currently possible. Currently, the FTC is not permitted to impose financial penalties on most first time offenders. These changes would help better incentivize companies to protect consumer security and privacy.<sup>30</sup>

### 3. Law Enforcement Access

Provisions of the Electronic Communications Privacy Act (ECPA) are imposing hard-to-justify barriers on foreign governments' ability to access communications content, such as emails, critical to their own investigations of serious crime—simply because the data happens to be U.S.-held. This is true even if the foreign government is investigating its own national in connection with a local crime and the *only* U.S. nexus to the data is that it happens to be held by a U.S.-based company in the United States. Instead, the foreign government is required to go through the mutual legal assistance process and initiate a diplomatic request for the data.

Consider, for example, U.K. law enforcement investigating a London murder spree. The U.K. officials seek the data of the alleged perpetrator in order to help establish motive. If the perpetrator uses a U.K.-based provider, the officials could access the data within days if not sooner. But if instead he uses a U.S.-based service provider, the U.K. officials are told that they must make a request for the data through the U.S. government, employing the mutual legal assistance treaty (MLAT) process—a laborious and time-consuming process that generally takes multiple months, sometimes years.<sup>31</sup>

---

*Tech.*, 114 Cong. 1 (2015) (testimony of Marc Rotenberg, President, Electronic Privacy Information Center) (calling for the adoption of a Consumer Bill of Rights).

<sup>30</sup> See Tara Siegel Bernard & Stacy Cowley, *Equifax is Facing Scrutiny. If Only it had Come a Bit Sooner*, N.Y. TIMES (Sep. 9, 2017) (noting that just last month, for example, the FTC punished TaxSlayer, a tax preparation service, yet lacked the authority to issue any fines because it was a first-time compliance action); Daniel J. Solove & Woody Hartzog, *The FTC and the New Common Law of Privacy*, 114 COLUM. L. REV. 583 (2014) (providing an excellent and thorough account of the privacy jurisprudence of the FTC).

<sup>31</sup> See, e.g., RICHARD A. CLARKE ET AL., PRESIDENT'S REV. GRP. ON INTELLIGENCE & COMM'C'N TECH., LIBERTY AND SECURITY IN A CHANGING WORLD 226-29 (2013), [http://www.whitehouse.gov/sites/default/files/docs/2013-12-12\\_rg\\_final\\_report.pdf](http://www.whitehouse.gov/sites/default/files/docs/2013-12-12_rg_final_report.pdf) (noting that the United States takes an average of ten months to respond to official requests made through the MLAT process for email records).

Foreign governments are understandably frustrated. And they are being incentivized to support data localization requirements in response—thereby ensuring access to sought-after data without having to go through the MLAT process.

Draft legislation sent to the Hill initially by the Obama administration and then again by the Trump administration would begin to address this problem. The legislation would amend ECPA so that foreign governments can, in specified and narrow circumstances, directly compel the production of communications content from U.S.-based providers, so long as baseline substantive and procedural protections are in place. This kind of direct access would only be available to those countries that entered into executive agreements with the United States; would continue to require use of the mutual legal assistance process if the foreign government were accessing the data of U.S. citizen or legal permanent resident or anyone located in the United States; and would require reciprocal rights of access to the United States in cases where it is seeking foreign-held data.

Moreover, the legislation includes a number of specific criteria designed to protect privacy and civil liberties. Among other requirements, the requests would have to be particularized, targeted, based on articulable and credible facts, and subject to judicial review or oversight; non-relevant information must be segregated, sealed, and deleted; and protections must be in place to ensure that the requests are not used as a means of acquiring information about a U.S. citizen or resident. There is room for some of these requirements could be strengthened, but in general they provide a notable set of baseline protections.

The criteria are sufficiently stringent that, at least initially, only a handful of countries would likely meet the requirements necessary to enter into the kind of executive agreements envisioned. As a result, it will not be a total panacea to the law enforcement-related concerns that are incentivizing data localization mandates around the globe. Nor should it be understood as such. But it would help disincentive data localization efforts with those countries with which the United States entered into the requisite executive agreements. And over time, it would establish a model—and baseline standards—that could be adopted more widely. It is legislation that Congress should, with some modest improvements, move quickly to adopt.<sup>32</sup>

#### 4. Protectionism and Free Trade

The United States can and should make the maintenance of a free and open Internet, pursuant to which data flows freely across borders, a centerpiece of its trade agenda. Here, I focus on three key efforts that the United States should pursue in this

<sup>32</sup> See also *Law Enforcement Access to Data Stored Across Borders: Facilitating Cooperation and Protecting Rights*, S. Judiciary Comm. (2017) (testimony of Jennifer Daskal, Professor, American University Washington College of Law), <https://www.judiciary.senate.gov/imo/media/doc/05-24-17%20Daskal%20Testimony.pdf> (describing draft legislation in more detail); Jennifer Daskal, *Law Enforcement Access to Data Across Borders: The Evolving Security & Rights Issues*, 8 J. NAT'L SECURITY L. & POL'Y 473 (2016).

regard.

*First*, the United States should leverage trade agreements to both eliminate and prevent barriers to data flows across borders. The now-defunct Trans-Pacific Partnership, for example, included a set of provisions would have prohibited mandatory data localization requirements. Similar and even stronger provisions should be included in other trade agreements as well.

*Second*, Congress should push the executive branch to continue to track digital protectionism and forcefully advocate the free flow of data in its bilateral and multilateral interactions, separate and apart from the treaty process. The placement of so-called digital trade officers in a handful of U.S. embassies is a start; this type of digital diplomacy should be expanded and encouraged.

*Third*, Congress should also push the administration to, when appropriate and preferable as part of a multilateral effort, initiate actions against those countries that are violating free trade obligations. More specifically, it should work to establish the important principle that data localization requirements violate free trade principles.<sup>33</sup>

### Conclusion

The free flow of data is good for privacy, security, and economic growth both domestically and globally. Yet, countries around the world are implementing a range of policies designed to restrict the free flow of data—in many instances pointing to U.S. policies and practices as a justification for doing so. Stemming this trend will require a multi-pronged strategy designed to address the privacy and security concerns expressed by foreign governments while also taking steps to stem the protectionist impulses that contribute to these trends. Doing so will be good for the economy, good for security, and good for privacy—both domestically and globally.

---

<sup>33</sup> See Nigel Corey, *Cross-Border Data Flows: Where are the Barriers, and What Do they Cost?*, INFORMATION TECHNOLOGY & INNOVATION FOUNDATION 13-17 (May 2017), [http://www2.itif.org/2017-cross-border-data-flows.pdf?\\_ga=2.65050406.927448598.1504895329-310094596.1504895329](http://www2.itif.org/2017-cross-border-data-flows.pdf?_ga=2.65050406.927448598.1504895329-310094596.1504895329) (making similar and additional recommendations).

Mr. LATTA. Well, thank you very much for your testimony. And, Mr. Reed, you are recognized for 5 minutes. Thank you.

#### STATEMENT OF MORGAN REED

Mr. REED. Thank you.

Chairman Latta, Ranking Member Schakowsky, and distinguished members of the committee, my name is Morgan Reed, and I serve as the president of The App Association, which represents 5,000 small business app makers and connected-device companies across the globe. Our members leverage the connectivity of devices from cars, to phones, to refrigerators, to produce innovation that enhances our lives.

The app ecosystem is now valued at roughly \$143 billion and represents the front end for \$8 trillion of international trade. Impressively, the big numbers produced by this powerful engine are actually driven by small businesses. Our members range from one-person shops with a few hundred people at the most. Yet virtually all of our members are global businesses with customers and users around the world. And small business in America is busy creating 64 percent of new private sector jobs.

The United States leads in world digital innovation. Why? Because American companies are at the forefront of using data to improve the lives of our customers. With over 7 million tech sector jobs, as you have heard from all of us on this panel, and a growth rate of 3 percent, the policy environment of the U.S. has produced successful tech industry, and countries all over the world are working to expand their tech sectors as well.

We must take steps to ensure continued job growth in the industry, and we see three key barriers. Nontariff digital trade barriers result from domestic policies rooted in privacy, some that require data localization; conflicts between U.S. law enforcement agencies' access to data stored overseas, which can and should be addressed with the passage of the International Communications Privacy Act, or ICPA. And I want to recognize Vice Chairman Harper as one of the cosponsors of that bill as well as full committee Chairman Walden, who is not here. And I want to thank you for your support on that important bill. We are looking to get Chairman Latta to support it as well.

And then, finally, any actions that weaken IP protections either through arbitrary enforcement of the law or through domestic sourcing preferences.

Everyone in the room understands the way data is a key aspect of how we use and benefit from the internet. We heard about the billions of dollars flowing across the border in terms of general commerce. But I would like to discuss some aspects of cross-border data that you might not have considered.

The future of medicine is in data that helps doctors make the right decisions. Think of it this way. You go to a physician, and a successful physician might have seen 25,000 patients by the time that they see you. But they have only seen about 500 with your genotype, age, gender, comorbidity, racial history, et cetera, et cetera. Now, imagine that the doctor can use data to know that, for example, a woman of Irish descent responds better to one medica-

tion and South Asian males under the age of 30 respond better to another. But we can only provide that kind of leap forward if we have data, including global data, about treatment and effectiveness.

And this isn't a pipe dream. In your district, Congressman Harper, the University of Mississippi Medical Center is relying on remote patient monitoring and digital data collection to provide tens of thousands of underserved in the state, and they rely entirely on technologies developed by our members and platforms.

Chairman Latta, in your district you have NAMSA, a leading medical research organization, and they rely on the Privacy Shield to interact with data from researchers around the world.

And an issue that I know Congresswoman Dingell knows well, the next advances in car safety technology will rely on access to data. Self-driving cars will run on data to tell the difference between a tree and a bicycle. And yet if we have foreign governments or our own government interfering with that cross-border data flow, we will block that key resource, which will harm our ability to save lives.

And it isn't all about life saving. Sometimes we just do it to make our lives easier. In Congressman Schakowsky's district, we have Paylocity, which helps manage software on the web for international clients to handle HR, payroll, and more.

Congressman Guthrie, in your district we have Hitcents, which is an innovative mobile apps and games company. And yet they are a global player with global customers.

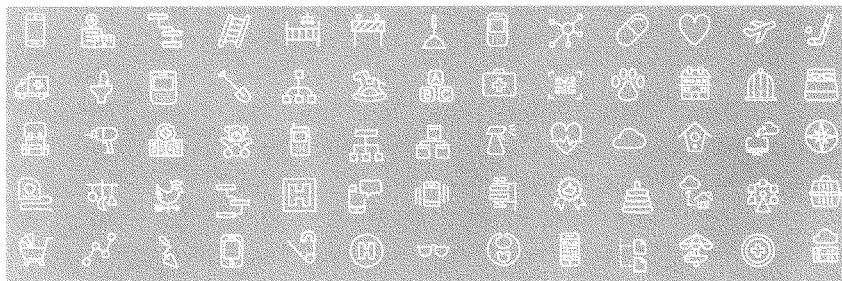
Congresswoman Clarke, we have got Brooklyn Software Dev that does web development applications and mobile applications. Again, it is a global company in your district with five people.

Congresswoman Matsui, you have got Health Rescue in your district. They are looking to expand internationally, and yet worries about cross-border data flow are harming their ability to get bigger, stronger, and do a better job for their patients.

In order to keep all of this going, we need Congress to act, and we need them to focus on the three key elements that you have heard from all of us today. We need to resolve the questions about law enforcement access. We need to resolve the questions about how we deal with intentional or other digital barriers to trade that serve as protectionists. And then, finally, we need to remember that my members' most valuable resource is often the intellectual property that is the engine behind their products.

I look forward to your questions, and thank you very much for this hearing.

[The prepared statement of Mr. Reed follows:]



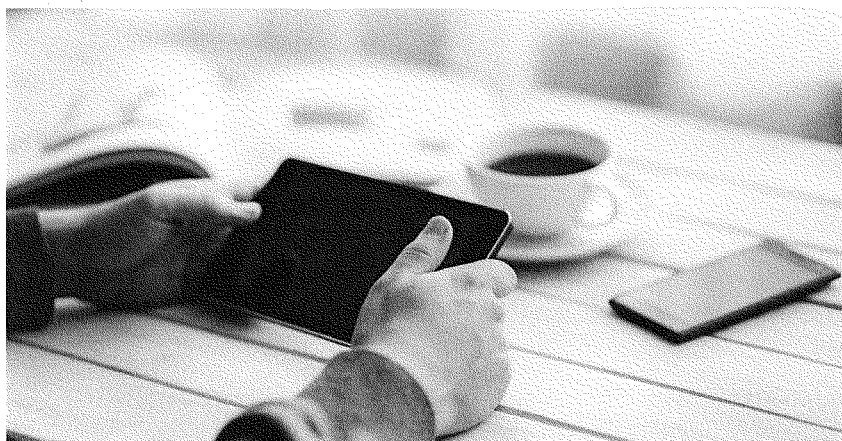
Testimony  
of Morgan Reed  
President  
ACT | The App Association

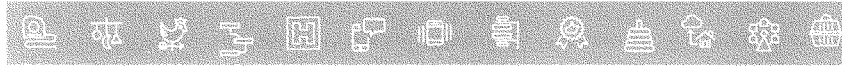
on

*"21st Century Trade Barriers: Protectionist Cross Border Data Flow Policies' Impact on U.S. Jobs"*

before the  
House Committee on Energy and Commerce  
Subcommittee on Digital Commerce and Consumer Protection

October 12, 2017  
2123 Rayburn House Office Building





### Executive Summary

Chairman Latta, Ranking Member Schakowsky, and distinguished members of the Subcommittee: My name is Morgan Reed, and I serve as president of ACT | The App Association, which represents about 5,000 small business app makers and connected device companies across the globe. Our members leverage the connectivity of devices--from cars to phones to refrigerators--to produce innovations that enhance our lives.

The app ecosystem is now valued at roughly \$143 billion, and represents the front end for \$8 trillion in international trade annually. Impressively, the big numbers produced by this powerful engine are driven by small enterprises.

Most of our members range from one-person shops to a few hundred people at the most. Yet virtually all our members engage in international trade. This is what gives us a unique voice on digital trade issues.

The United States leads the world in digital innovation. Why? Because American companies are at the forefront of using data to produce beneficial services. With over seven million tech sector jobs, and a growth rate of 3 percent, the policy environment in the U.S. has produced a successful tech industry, and countries all over the world are working to expand their tech sectors as well. We must take steps to ensure continued growth for the industry.

### We see three main barriers to continued success:

- Non-tariff digital trade barriers that result from domestic policies said to be rooted in privacy, national security, law enforcement, or similar interests;
- Efforts in international forums to restrict cross-border data flows; and
- Conflicts between U.S. law enforcement agencies' access to data stored overseas and foreign laws, which could be ameliorated with legislation such as the International Communications Privacy Act (ICPA) (H.R. 3718).

7 million U.S.  
tech sector jobs; growth  
rate of tech sector:  
**3 percent**

Digital trade supports American jobs, and it can also save lives. The future of medicine is in data and artificial intelligence. A successful physician might see about 15,000 patients throughout her career, but recent innovations in technology have grown doctors' reach and effectiveness exponentially. Our members create data-driven platforms that enable doctors to make decisions based on hundreds of thousands, even millions, of examples. For instance, with these software tools, a doctor can plug in a patient's characteristics and see which medication is most likely to work. These advantages benefit everyone, and yes, they can save lives. But they can only exist when data is accessible. Our member companies know that policies that stop data at national borders seriously degrade these life-saving capabilities.

### App Ecosystem:

currently valued at  
\$143 billion, \$8 trillion global  
market for internet of things  
over the next decade



In an example this Subcommittee knows all too well, the United States faces more than 35,000 traffic fatalities every year, the majority of which are due to human error. However, with the right technological advances, lives will be saved. Airbags, safety belts, and other innovations helped reduce traffic fatalities from a high of nearly 55,000 in 1972. But the next advances in safety technology will depend on access to international data. Self-driving cars will run not just on energy, but also on data from drivers and traffic patterns from around the globe. How can a self-driving car recognize a bicycle or a cyclist? How does it know the cyclist is not a tree? The machine-learning engine that cars use must have seen bikes in all their forms, in millions of different contexts. The United States simply cannot provide all the scenarios self-driving cars will encounter, therefore American car companies, especially those that sell in overseas markets, must perform testing overseas that depends on the cross-border transfer of data. When foreign governments enact policies that encumber the flow of data overseas—some going so far as to directly require the localization of data—they are blocking U.S. companies from using a key resource, not just to create jobs, but also to save lives.

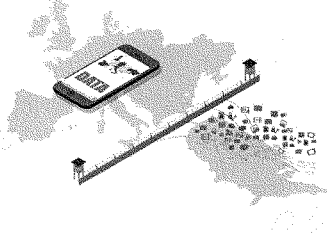
Some barriers to cross-border data flows are direct and intentional, and others are unintentional consequences of domestic priorities. We are working hard to educate foreign governments on the effects their domestic policies could have on cross-border data flows. We urge American policymakers to look to trade agreements as a tool to help ensure the policies intended to protect privacy do not unduly burden cross-border data flows and hurt U.S. job creation.

As American trade negotiators work to preserve the digital economy, Congress should consider updating key statutes to remove conflicts with other sovereign laws. Among other things, ICPA would reduce crippling legal uncertainty for our members and American companies looking to do business overseas. It would also provide cover for American trade negotiators as they seek to show foreign governments that our privacy protections are equal to theirs.

The digital economy is steadily growing more important in our trade relationships, giving rise to numerous actions by foreign interests that have serious consequences for American businesses. Many of the battles we are fighting today feel like déjà vu—they are remarkably similar to the issues this Subcommittee highlighted three years ago. As these trends continue, our trade relationships present the best opportunity to stop digital protectionism abroad and protect economic growth and job creation at home. I look forward to a discussion about how we can accomplish these goals, and working with the Subcommittee on these issues in the future.

### **I. American Small Business Innovators Face Numerous Barriers to the Free Flow of Data Across Borders**

Foreign governments seek to encumber the free flow of data across political boundaries for many reasons and in a variety of ways. While some of these policies are based on legitimate goals (e.g., to protect privacy rights or public safety), they are often thinly veiled efforts to protect domestic industry. Previously-negotiated language to address these policies would require signatory countries to “allow the cross-border transfer of information by electronic means, including personal information . . .,” one of many landmark provisions poised to assist the growth of the digital economy. The App Association continues to urge the U.S. Trade Representative (USTR) to include this clear protection of cross-border data flows in any update to the North American Free Trade Agreement (NAFTA)—to ensure American businesses in the digital economy may access the Canadian and Mexican markets more easily, and to serve as a standard for future trade agreements.





### **a. Frequency of Data Localization Requirements Limits U.S. Small Business Innovators' Ability to Grow**

The required siting of data centers and digital infrastructure—and mandates to store data—inside of a country's borders harms the free flow of data across borders. These policies serve as a direct barrier to market access, and ignores the efficiencies of cloud computing. Previous multilateral agreement language sought to address these problematic proposals with a provision prohibiting member countries from requiring companies to "use or locate computing facilities" inside that country's borders, with limited exceptions. We support NAFTA, currently being re-negotiated between the United States, Canada, and Mexico, and encourage the inclusion of similar provisions to provide a predictable policy across North America, and a strong signal to combat the growing number of data localization policies we see around the globe.

Numerous data localization requirements are in place today, actively locking American small businesses out of important markets. Key examples include:

China has either proposed or implemented numerous restrictions on the flow of data across its borders. These regulations limit or prohibit the transfer of data related to banking and financial credit, cybersecurity, counterterrorism, commercial information systems, healthcare, and insurance outside of China. These policies each represent a significant barrier to market entry and serve as a non-starter for small businesses that would otherwise look to China to expand their businesses and create jobs.

- Indonesia's Ministry of Communications and Information Technology (MCIT) requires electronic system providers for public services to locate a data center and disaster recovery center within Indonesia.<sup>2</sup> The European Centre for International Political Economy has estimated that Indonesia's use of data localization requirements, in this context and others, will result in a 0.7 percent loss in its gross domestic product.<sup>3</sup>
- India's National Data Sharing and Accessibility Policy requires all data collected using public funds be stored within the borders of India.<sup>4</sup> In addition, India's 2015 National Telecom M2M ("machine to machine") Roadmap,<sup>5</sup> which has not been implemented, states that all M2M gateways and application servers serving customers in India must be located within India. The draft policy also proposes rules that prohibit the use of foreign SIM cards in devices in India.
- Russia's Federal Law No. 242-FZ, signed by President Vladimir Putin in July 2014, requires companies that store and process the personal data of Russian citizens to maintain servers on Russian soil, and to notify the federal media regulator, Roskomnadzor, of all server locations.<sup>6</sup> This law empowers Roskomnadzor to block websites and to maintain a registry of data violators.
- Turkey's E-Payment Law mandates the processing of e-payments must occur within Turkey.<sup>7</sup> In mid-2016, Turkey's Banking Regulation and Supervising Industry (BDDK) initiated a policy that requires companies to locate their ICT systems in Turkey.<sup>8</sup> These data localization requirements have jeopardized our members' plans to enter this important market should their app include e-payment capabilities.
- Nigeria has implemented even harsher data localization policies, not only requiring companies to store their data within Nigeria, but also mandating that at least 50 percent of any information or communications technology devices manufactured in the region be comprised of locally sourced inputs.



Data localization requirements are being implemented at an alarming rate that continues to grow. Our members rely heavily on cloud computing and its efficiencies, but these policies create significant barriers and untenable burdens. The ability to use cloud service providers to store and process data has allowed our members and businesses of all sizes to compete in the global economy and reach consumers around the world. However, requiring the construction of new data centers, or the exclusive storage of data in a country, coupled with the inability to share data across borders hurts these opportunities for global engagement and success. American businesses need strong provisions in future trade agreements to combat these real and growing data localization policies. Now is a vital time for the United States to lead by example, both in domestic laws and our negotiated bilateral and multilateral trade agreements.

Similarly, our members encounter a growing number of policies that require the transfer of proprietary source code or encryption keys as a condition for market entry.<sup>9</sup> These policies are unacceptable for our members, and businesses of all sizes, because their intellectual property (IP) is the lifeblood of their innovation.

### **b. European Privacy Laws Are Particularly Burdensome for Small and Medium-Sized Companies**

Some countries' policies impede the international flow of data, and business, in unintentional ways. For example, various provisions of the General Data Protection Regulations (GDPR), set to go into effect on May 25, 2018, impose additional requirements on non-European firms that increase the cost and risk associated with handling data that may pertain to EU citizens. For example, Article 27 of the pending law requires firms to physically place a representative in the EU.<sup>10</sup> This can be an insurmountable hurdle to our small and medium-sized members entering the EU market. Anything that can be done during GDPR implementation to ease the burden for these small and medium-sized companies could have hugely positive economic implications.

The new GDPR requirements have also created conflicting obligations for foreign companies that abide by U.S. and other international laws. For example, the impact of the GDPR on the oversight and management of the global domain name system, currently implemented by the Internet Corporation for Assigned Names and Numbering (ICANN), is uncertain. The GDPR may jeopardize ICANN's effectiveness by inhibiting the transfer of information about websites that is necessary to protect consumers and intellectual property. This is not just an impediment to U.S. companies that provide critical Domain Name System (DNS) functions, but also to the broader digital economy that depends on their services.



### **c. Privacy Shield as a Model for Protecting Data While Facilitating Data Flows**

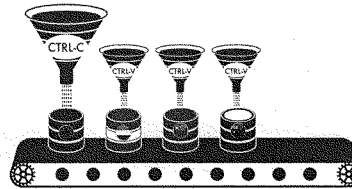
The recent trend of unilaterally imposed restrictions to cross-border data flows is damaging for businesses of all sizes. For instance, many governments are seeking to force data to reside within national boundaries by imposing data localization laws, strict licensing regimes, data retention requirements, government procurement regulations, and pressure on public sector sales. We urge policymakers to look to trade agreements as a tool to help ensure these sorts of detrimental policies do not unduly burden cross-border data flows and hurt U.S. job creation.



For example, the Privacy Shield framework between the EU and the U.S. offers a bilateral cross-border data transfer framework that could be a model for other jurisdictions concerned about protecting personal data leaving national borders.

Numerous App Association members have undertaken significant effort to meet the Privacy Shield's requirements and are today certified to the Privacy Shield. The U.S. government has also taken significant steps to hold up its end of the bargain by holding companies that certify to the Shield to account.<sup>11</sup>

As a result, we strongly believe the Privacy Shield provides protections that are "essentially equivalent" to those of European law, and support its continuation. The App Association has communicated this support directly to the EC at its invitation in July of 2017.<sup>12</sup> The first annual joint EU-U.S. review of the Privacy Shield is a landmark assessment that we are closely engaging with regulators about, on both sides of the Atlantic. Our small business members would be especially disadvantaged by the invalidation of the Privacy Shield.



## II. Ongoing Efforts to Expand the Scope of the International Telecommunications Union

International governmental organizations pose unique threats to the global digital economy. The International Telecommunication Union's (ITU) proposal contemplating a role for itself in over-the-top (OTT) services is particularly concerning. An agency of the United Nations (UN), the ITU allocates global radio spectrum, manages satellite orbits, and develops technical standards to ensure the interconnection of telecommunications. However, the ITU does not currently have a role in internet traffic or services.

The ITU's Council Working Group (CWG) has proposed an "Open Consultation" to gather comments from stakeholders about public policies pertaining to OTT services.<sup>13</sup> In general, OTT services refer to those that operate on the internet, including apps and websites.

Numerous data localization requirements are in place today, actively locking our American small businesses out of key markets. Key examples include:

Therefore, in concert with existing laws for companies that operate on the Internet, the imposition of specific regulations on OTT services would be redundant, and serve as additional barriers to trade.

While a proposal to examine public policies concerning OTT services may seem benign, a similar proposal in 2012 sought to expand the ITU's reach to include the regulation of internet services. The proposal was largely viewed as an international justification for heavy-handed regulation, partitioning, and censorship of the internet. The United States ultimately challenged the 2012 proposal during the World Conference on International Telecommunications (WCIT), and Representative Mary Bono, this Subcommittee's then-chairwoman, put forth a congressional resolution to allow the U.S. delegation to walk away from an ITU vote on the issue.<sup>14</sup>

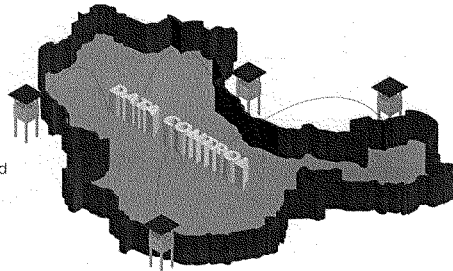


The ITU's current proposal is just as threatening. Expanding ITU's reach to include OTT services would represent the UN's intervention into general online commerce policy, and could easily result in the arbitrary taxation of internet traffic on a country-by-country basis. The App Association filed detailed comments opposing the ITU's expansion into OTT services and presented our argument to ITU member state delegations in Geneva, Switzerland, last month. We also served as a sector expert for the U.S. delegation to the ITU's working group on Internet Governance, where we reinforced these viewpoints to ITU staff and member states.

We believe the Subcommittee should closely monitor, and consider engagement in, OTT-related developments in the ITU, and vigilantly seek opportunities to bolster the U.S. bargaining position in bilateral, multilateral, and international contexts. We believe a resolution in line with Representative Bono's could help prevent mission creep at the ITU. We remain committed to working with this Subcommittee to advance U.S. interests in the ITU, and to keep the ITU's efforts within its remit.

### III. Conflicts Between Domestic and Foreign Data Access Laws

Cloud computing has enabled American app developers to securely access, share, and store the 2.5 quintillion bytes of data created daily to better serve consumers across the globe. Unfortunately, the Electronic Communications Privacy Act (ECPA), the statute governing law enforcement's access to stored data, was written in 1986, long before the advent of cloud computing, and does not clearly outline when and how law enforcement can access data stored overseas. Several U.S. courts have contradicting interpretations of ECPA's reach, and many have concluded that ECPA's scope is so broad that it directly conflicts with other countries' domestic laws. While these differing legal conclusions remain unresolved, many law enforcement agencies continue to use ECPA to authorize requests for data pertaining to citizens of any country, stored in any country. As companies increasingly store data on servers around the world, this creates serious uncertainties for their operations and success.



Compliance with a law enforcement request that conflicts with domestic laws could, in some instances, result in a penalty of up to 4 percent of global revenue for a company. In these cases and others where a conflict exists between domestic and foreign law enforcement statutes,<sup>15</sup> our members are stuck between a rock and a hard place, or left with a significant financial burden. The confounding legal uncertainty undoubtedly establishes a non-tariff barrier to digital trade—it requires substantial capital and legal resources that small businesses like our members simply cannot bear.

Nonetheless, the App Association favors the reform of intelligence surveillance and criminal investigation statutes, and strongly believes Congress should reform ECPA. The App Association deeply appreciates the House of Representatives' unanimous passage of the Email Privacy Act (H.R. 387) earlier this year. However, more must be done to ensure U.S. companies doing business abroad do not face conflicts between law enforcement requests and foreign laws. We believe ICIPA (H.R. 3718) legislation would ameliorate conflicts between foreign laws and U.S. law enforcement agencies' authority to obtain data pertaining to foreign citizens, and help remove this trade barrier.



#### IV. Intellectual Property Rights and Competition Law

Every year, app makers and content creators lose an estimated \$3 to \$4 billion from the installation of roughly 14 billion pirated apps globally.<sup>16</sup> Several foreign governments continue to use competition law to propose and enact policies that seek to extract, or make it hard to protect, U.S. companies' valuable intellectual property. The strong protection of IP is crucial to our members' ability to do business overseas.<sup>17</sup>

#### V. Conclusion

This Subcommittee has a strong history of bolstering digital trade priorities. We are heartened by the continued focus on these issues, but the stakes are higher today than when the Subcommittee last examined these issues three years ago. An ever-growing number of American jobs depend on digital trade, while the interests that support digital protectionism are becoming more influential. We have much more work to do to protect the vitality and dynamism of the digital economy, and we look forward to working with you in these shared endeavors.

1 Art. 14.11, TPP (2015) found here: <https://ustr.gov/sites/default/files/TPP-Final-Text-Electronic-Commerce.pdf>.

2 See Mary R. Silaban, *Unleashing Indonesia's Digital Innovation*, American Chamber of Commerce in Indonesia (June 10, 2014), available at <http://www.amcham.or.id/4614-unleashing-indonesia-s-digital-innovation>. See also, U.S. Dep't of State Bureau of Economic and Business Affairs, *2014 Investment Climate Statement – Indonesia*, (June, 2014), available at <http://www.state.gov/documents/organization/226821.pdf>.

3 [http://www.ecipe.org/app/uploads/2014/12/OCC32014\\_1.pdf](http://www.ecipe.org/app/uploads/2014/12/OCC32014_1.pdf)

4 Government of India Ministry of Science & Technology, *India's National Data Sharing and Accessibility Policy*, (2012), Available at <http://oggit.gov.in/NDSP/NDSP-30Jan2012.pdf>.

5 Government of India Ministry of Communications & Information Technology Department of Telecommunications, *National Telecom M2M Roadmap*, Available at <http://www.gama.com/connectedliving/wp-content/uploads/2015/05/150513-DoT-National-Telecom-M2M-Roadmap.pdf>.

6 Russian Federation, *Federal Law No. 242-FZ*, (July 21, 2014), available at <https://pd.rkn.gov.ru/authority/p146/p191/>.

7 U.S. Dep't of State Bureau of Economic and Business Affairs, *2016 Investment Climate Statement – Turkey* (July 5, 2016), Available at <http://www.state.gov/e/eb/rls/oth/ic/2016/eur/264425.htm>.

8 Turkey's Banking Regulation and Supervising Industry (BDDK), *Law on Payment and Security Settlement Systems, Payment Services and Electronic Money Institutions* numbered 6403, Official Gazette numbered 28690, (published June 27, 2013), Available at [https://www.bddk.org.tr/web/sites/english/Legislation/12916493kanun\\_ing.pdf](https://www.bddk.org.tr/web/sites/english/Legislation/12916493kanun_ing.pdf).

9 See <https://actonline.org/wp-content/uploads/MET-Pre-Installed-App-Regulation-.pdf>; <http://www.worldpolicy.org/journal/fall2013/Russia-surveillance>.

10 <https://www.privacy-regulation.eu/en/27.htm>

11 <https://www.ftc.gov/news-events/blogs/business-blog/2017/09/ftc-cases-affirm-commitment-privacy-shield>

12 [http://actonline.org/wp-content/uploads/07062017\\_App-Assn-Ltr-re-EU-US-Privacy-Shield.pdf](http://actonline.org/wp-content/uploads/07062017_App-Assn-Ltr-re-EU-US-Privacy-Shield.pdf)

13 <http://www.bu.int/en/council/cwv-internet/Pages/consultation-june2017.aspx>

14 <https://www.congress.gov/112/bills/hconres/127/BILLS-112hconres127rfs.pdf>

15 See <http://ehoganlovelis.com/cv/92a5428dc5d8947a6ef3abd4eb68b549ae2472b>

16 <https://www.forbes.com/sites/patrickcoetsier/2017/07/24/app-developers-losing-3-4-billion-annually-thanks-to-14-billion-pirated-apps/#607b170490da>

17 The App Association is advising USTR on its investigation into China's intellectual property protection policies.

Mr. LATTA. Well, thank you very much. And as the gentlelady from California said to me, you did your homework on us. Thank you very much for your testimony today.

And, Mr. Garfield, if I could start my questions with you. How do the restrictions on cross-border data flows not only impact industries like yours in the technology sector but others like manufacturing, retail, energy, and healthcare?

Mr. GARFIELD. Thank you for the question. As all of the witnesses have shared, cross-border data flows, digital trade, is a broad economic issue. And so whether you are in farming or pharmaceuticals, you rely on cross-border data flows for your companies to function.

Moreover, it is no longer a big company versus small company issue. As Mr. Reed pointed out, there are small companies in all of your districts that rely on this. And so it is, in fact, in our economic interest to make sure that there aren't restrictions that limit the growth of those companies.

Mr. LATTA. Thank you.

Ms. Espinel, can you discuss how big data cloud computing, artificial intelligence, and other emerging technologies like blockchain are changing how business is done, and why cross-border data flows are important for these disruptive technologies and future innovation?

Ms. ESPINEL. I would be happy to. So artificial intelligence, by its nature, typically demands large amounts of data in order to learn from that data and help whoever is using it, whether it is a doctor or a farmer or a manufacturer, be able to make better decisions based on that data. Artificial intelligence, in most circumstances, doesn't really work unless there is a large amount of data. And if you are trying to discern patterns or the best outcome, having as much data from as many places in the world is very helpful. And I will give a specific example of that.

But first you mentioned data analytics. Data analytics is often a little bit like looking for a needle in a haystack. So you have, typically, very large, unstructured datasets. And what data analytics is letting you do is discern meaningful patterns that will then, again, help you make better decisions that would be virtually impossible, or literally impossible, for human beings to do on their own. But artificial intelligence, data analytics, are two examples of things that really don't work, unless you have very large amounts of data and the computing power to be able to process and analyze it coming from various places around the world.

To make that a little bit more concrete, I would turn to agriculture as one of the many, many, many examples of sectors that are using it. So many farms now have sensors in the soil. Those sensors, among other things, are determining the levels of moisture that are in the soils. And farmers can take the data that they are getting from the sensors that they are planting in their own farms and they can compare it to historical weather patterns around the world. And they can then use that to make decisions about when is the best time to plant, how best to irrigate, when is the best time to harvest. Their ability to do that is totally dependent on the ability to gather historical data on weather patterns across the world.

It doesn't work, it doesn't give them the same advantage, unless they have the ability to do that.

I will mention one other example, which I think is very much on people's minds today, which is cybersecurity. Cybersecurity and companies' ability to be able to protect themselves from threats is—I am trying not to be overly superlative because that is not in my nature. But it is incredibly enhanced, shall we say, by the ability to be able to detect patterns of threat that are moving around the world in realtime. And you cannot do that unless you have access to the data from around the world.

It also allows companies internally to be able to look at their network analytics and how they are using technology inside their own companies, and then, again, compare that to threat data that they are collecting from around the world. That is, again, quite literally not possible, unless you have the ability to collect data from around the world and to do it in realtime, which means you need to be able to do it with as little friction as possible.

I think myself and every member of this panel could give you examples in manufacturing and agriculture and healthcare and financial services. So I will yield back my time to others if they want to. But the examples are plentiful. And I think what is really exciting is that, as plentiful as they are, we are also clearly at the beginning of what is possible. We talk a lot about data revolution and how that is transforming business and transforming the economy. But we sometimes forget that that itself is very nascent, and I think the advances that we are going to see over the next 5, 10, 20 years are going to dwarf the advances that we have already seen so far, as long as the ability to transfer data across borders remains.

Mr. LATTA. Thank you.

Mr. Reed, in my remaining time, again, you pointed out a lot of the small businesses that you represent. And one of the other major concerns for the small business is small, medium enterprises that do not have the resources to localize this data production or facilities in a country abroad. How do they go about it?

Mr. REED. Well, I think as you have heard from all of us, the revolution of data often is primarily aided by the concept of cloud computing. We all know that the term "cloud computing" is a bit of a marketing term, but the idea that data can be anywhere and everywhere all at the same time is absolutely critical to a small business.

So data localization laws that go into effect in other parts of the world, which limit two aspects: One is data localization laws that say any data collected on a citizen of that country must be on a server and only be on a server in that country. That is terrible. It is almost impossible to grow in that kind of an environment as an American company.

And the second is one that you have heard all of us talk about, is the future of what this can do to improve lives. Now, imagine that I can't take that data out or I can't use it. I can't bring it back to the United States to analyze it. I have to set up a whole series of different cybersecurity mechanisms based on the state or national laws in those other countries. And all of a sudden, if I am a small business, and I am looking in my pocketbook and thinking,

do I hire a developer to work on a product here in the states or do I roll the dice and spend a fortune to do something in a country where I don't speak the language, I no longer can depend on the cloud, and I no longer have the resources in place to grow, then they are going to opt out of that global opportunity. And when they opt out of the global opportunity, they opt out of creating more jobs here domestically.

Mr. LATTA. Well, thank you very much. And my time has expired.

And I would like to recognize the gentlelady from California for 5 minutes.

Ms. MATSUI. Thank you very much, Mr. Chairman. And thank you very much for calling this very important hearing today. And I want to thank the witnesses for joining us today. This has been a very interesting discussion.

Dr. Daskal, it is clear that while many data flow policies across the world are blatantly protectionist, countries also have real privacy issues to address. How can we distinguish between policies that are purely protectionist and those that address a legitimate need?

Ms. DASKAL. So thank you, and thank you for the question.

As I said in my testimony, I think that the factors motivating data localization are multiple, and it is not always possible to parse out what is the motivating factor. And it highlights, I think, the need to work on the various different areas that identify both dealing with trade policy and concerns about the digital efforts to be protectionist.

At the same time, there are a number of data localization mandates and data localization rules that derive from concerns about U.S. privacy protections, both consumer privacy protections and also concerns about the scope of U.S.-foreign intelligence surveillance. And addressing those, I think, is also critical, particularly with respect to preserving the flow of data from the EU to the United States.

As we have talked about, the Safe Harbor Framework that was in place was struck down primarily because of concerns about the scope of foreign intelligence surveillance. And there are now a number of court cases, including one that was just referred back to the European Court of Justice, that raises those same set of concerns based on a record and a finding by the Irish High Court that said we have a lot of concerns about the scope of U.S.-borne intelligence surveillance and the sufficiency of remedies for EU citizens whose data is collected.

Ms. MATSUI. OK. Mr. Garfield, in your testimony, you say that even when governments have the right motivations, like protecting public safety and privacy, they often pursue the wrong policies that result in data flow barriers. What do you see as the right privacy and public safety policies that will not impede data flows?

Mr. GARFIELD. I think a part of what is needed here is actually U.S. leadership in bringing the world along in developing definitions. And so I could sit here today and give you my sense of what the appropriate data security or privacy regime should look like. But I think the U.S. has an opportunity to build on the Privacy

Shield in a way that is globally necessary and encouraging. And so that is what I would actually encourage.

Ms. MATSUI. OK.

Mr. GARFIELD. It is bilateral in the sense that it is with the EU and all of the countries of the EU. But we have an opportunity to build upon that with the rest of the world. And the way that data moves today, it is absolutely necessary to do that on a global basis.

Ms. MATSUI. All right. OK.

Just yesterday, the President suggested he could support breaking up NAFTA into separate, bilateral trade agreements.

Dr. Daskal, do you think breaking up NAFTA or other multilateral agreements will have any impact on our efforts to ensure the global-free flow of data? If so, how?

Ms. DASKAL. So I would be concerned about an effort to break up NAFTA. I think we have heard from other panelists the importance of NAFTA and the importance of using NAFTA as an opportunity to promote a digital-free trade agenda. And I hope that the administration follows the recommendations of all of those who support that quite strongly.

Ms. MATSUI. OK. And I have been very concerned about the forced transfer of technology as a condition for foreign market access, especially as it pertains to encryption and intellectual property. Can any of our witnesses provide examples of these forced transfers? And do you have any suggestions of how we might address this issue? Any of you?

All of you can comment.

Ms. ESPINEL. So, yes, I think there are specific countries around the world where we have seen either our members not be able to access the market or have their access severely limited. And among those are Russia, Indonesia, Brazil, China, Vietnam. Mr. Garfield noted many of these as well. And we have concerns that the litigation that Ms. Daskal and I believe other of the panelists have referred to several times, the litigation that is happening right now in the European Union, is also going to end up limiting data flows between the United States and Europe. So this is a live issue in many parts of the world.

I think in terms of what can be done, a part of that is Congress continuing to encourage the administration to tackle this issue head-on. I do think, at least in our interactions with the Department of Commerce and with USTR, they realize how important digital trade is to the United States and to the global economy, but it is not an easy issue. So I think continuing to make clear to them that this is also a priority issue for this committee is very important.

We live in a world right now where we don't have any international consensus on what the right set of rules would be. You have heard many of us talk about NAFTA. A big part of the reason that we are interested in NAFTA is because it gives an opportunity to start setting that precedent, and that is really where we need to go to collectively. We need to have, at least among the major economies, an international consensus on what the right sets of rules around free movement of data should be. And that does not exist right now.

Mr. GARFIELD. If I may just suggest one recent report. The Information Technology and Innovation Foundation is doing an annual report on cross-border data flows and the limitations to that. In that report, they identified 37 countries that now have these principles in place or limitations in place. And so we can make that report available for the committee as well.

Ms. MATSUI. OK. Well, thank you very much.

And Mr. Chairman has been very generous with me. So I need to yield back. Thank you.

Mr. LATTA. Well, thank you very much. The gentlelady yields back.

The chair now recognizes the gentleman from Mississippi, the vice chairman of the subcommittee, for 5 minutes.

Mr. HARPER. Thank you, Mr. Chairman. And thanks to each of you for being here.

It is mind boggling when you think of where we are today and with the opportunities that we have. And think back 10 years ago, I don't know that we could have envisioned we would be on the—with such opportunities. And the challenges really are opportunities for us.

And so I want to thank you each. You bring so much expertise to the table to help us as we go forward to make sure that we do things that do improve people's lives, that we do things that don't block that cross-border flow. And we want to make sure that we get it right. And, certainly, there are those opportunities we are going to grasp and go forward.

So, Ms. Espinel, you mentioned in your testimony that you indicated how digital trade can improve lives. Explain to me how that works. When I go back to my home State of Mississippi, what should I tell them?

Ms. ESPINEL. So I think Mississippi, as we have already heard today, is a leader in healthcare and in personalized healthcare. And I think that is an area that is well worth emphasizing. So I am going to tell a story that is a little bit personal to me because it is borne out from my personal experience, actually in a couple of areas, where artificial intelligence and the ability to assess data from around the world is making an impact.

The first I will start with is Alzheimer's. So my mother suffers from Alzheimer's. Researchers in the United States and Japan and Europe are now working together using technology developed by IBM Watson to use the medical patterns of Alzheimer's patients from around the world to hopefully be able to find, if not a treatment to Alzheimer's, increase risk factors for Alzheimer's. And that is an issue that is personal to my family. I know it is an issue to many families around the world. I think anything we can do to advance there is well worth it. And, again, that is an area where it is, if you are restricted to your ability to use data from a specific population set, that is going to make it much, much slower to be able to see the kind of advances that we would like.

Another example that also resonates with me because of my own personal experience relates to doctors in Canada. So doctors in Canada started monitoring newborn babies, prematurely newborn babies for signs of risk. And one of the things that they found is that right before a premature baby has a crash, goes into a serious

risk incident, their vital signs stabilize, which is actually sort of intuitively very strange, right. So, in fact, the medical practice up to that point had been if they saw the vital signs stabilize, they would lessen the monitoring of that particular baby because the assumption was that the baby was going into recovery. What they actually found using cross-border data flows and data analytics, was that, in fact, that is a risk factor for a baby going into crisis. And that has completely changed the treatment and the monitoring of premature babies that are in the NICU and has saved lives.

As a mother who, happily for me, very briefly had a child in the NICU, that is an example that resonates—

Mr. HARPER. Sure.

Ms. ESPINEL [continuing]. With me very strongly. But it is another example of an advance that would have been literally impossible without the ability for doctors to be able to compare datasets from around the world.

Mr. HARPER. That is great.

Ms. ESPINEL. So Mississippi is a leader in healthcare. There are so many great examples there, and I think anything that we can do to try to keep the data within—while respecting privacy, to keep medical data flowing around the world to try to help researchers and doctors treat their patients is tremendous.

Mr. HARPER. Thank you very much.

Mr. Reed, we discussed a few moments before the hearing began, you know, University of Mississippi Medical Center selected last week as a Telehealth Center of Excellence. And that just didn't happen because they went around to pick that. Tell us how following up on that has helped.

Mr. REED. The reality is for University of Mississippi Medical Center, and I think there is something important. The ability to save lives is a critical aspect of this. But also, let's not undervalue the fact that the University of Mississippi is also looking for the students that are coming out of there, and the school itself, to create jobs, to create opportunities, and to break the place that they are now and find something that they can do. They can hire 10 people, 20 people, 30 people. And you start to look at the fact that, from UMMC, when they are looking to do spinoffs and those students are looking to build the next product that comes out of there, they are going to rely on data from all across the world to find that next solution. The example I gave you, if I have got to figure out what drug works better on this group of people versus this group of people, then I need the data to do so.

And so it is important that we find a way to solve the health problems that we have raised, but let's not undervalue the fact that part of what we are also doing is looking to promote entrepreneurship. And entrepreneurship comes from information. All of us in the business case, we talk about asymmetry, information asymmetry. We lose out when we have with information asymmetry. The more information they have, the better the product they can make, the more jobs that they can build. And I think we should remember that part of this is using data to spur entrepreneurship as well as life saving.

Mr. HARPER. Great. Thank you, Mr. Reed.

My time has expired, Mr. Chairman.

Mr. LATTA. Well, thank you.

The chair recognizes the gentleman from Vermont for 5 minutes.

Mr. WELCH. Thank you very much. I thank the panel of witnesses. We are on pretty good bipartisan terms here. And the reason is because what we are talking about, the data flow, is so important to the economy, independent of where you are from or even what your enterprise is.

And the two issues that I guess I want to ask about are, number one, what are some of the issues we have to deal with with respect to European actions that are intended either to protect privacy as they see it, somewhat different than ours, and the collateral consequences of the Snowden incident? And, number two, some of the anticompetitive steps they may take disguised as privacy steps for their people.

So I will start with you, Ms. Espinel. Can you address that?

Ms. ESPINEL. So I will mention at least two things. One is there is a regulation called the GDPR that is in the process of being implemented throughout Europe. And part of what the GDPR does is puts into place stronger privacy rules.

I will say, based on the experience at least of my companies, what we have found is, in terms of implementing that, U.S. companies are often far ahead of where the European companies are. So I think our companies, and certainly my members and their commitment to privacy, is unparalleled.

However, I think we do have concerns about some potential regulations or litigation challenges that are happening in Europe. So two I will highlight is there is an e-privacy regulation that is being discussed in Europe right now, and we do have concerns that that is going to make it very difficult to operate in Europe, while not actually advancing the cause of privacy very much. So that is one that I would flag.

The second I would flag is one that we have mentioned a couple of times on the panel, but I think it bears repeating because the threat of it is so serious. While the Privacy Shield is in place, as you know—and we were happy to see the United States and Europe come to an agreement and conclusion, and we are happy that it remains in place—the Privacy Shield is only one of the mechanisms that companies use for moving data back and forth and around the world. And the other challenge, there are other mechanisms called standard contractual clauses that are right now also being challenged in Europe, as Ms. Daskal referred to. Those have been very recently referred up to the European Court of Justice. Potentially, the impact of those being overturned could be even broader than the impact when the Safe Harbor was revoked. So we are watching that with great interest. And I think that goes to the discussion that we need to have collectively between the United States and Europe about what a long-term solution is.

Mr. WELCH. OK. Thank you.

Go ahead, Mr. Reed, and then Ms. Daskal.

Mr. REED. I think that one of the key elements that is on the forefront is finding a way to solve the question about law enforcement access. Right now, the International Communications Privacy Act, H.R. 3718, is going to be critical. Because we are staring right in the face of a decision by a court that will essentially say that

U.S. law enforcement can take data from anywhere, regardless on who it is on, regardless of what country it is stored on. And while that may be the right decision, the impact that that will have on our ability to do cross-border data flow with Europe will be significant. Because if we say that, then you have to assume that the European nations are going to say the same thing.

And then, without a comity agreement, without some kind of ability for companies to adequately provide for the security of that data, you are facing a world where U.S. companies are either going to have to obey the law of the United States and find themselves in violation of laws overseas or violate the law in the United States to serve their European customers. And nothing will do as much damage to our positive relationship with Europe than the idea that I can no longer do business there without breaking a law in one place instead of the other.

Mr. WELCH. Ms. Daskal, I have only got about a minute, a little less. Thank you.

Ms. DASKAL. So I fully agree that the issue of law enforcement access to data across borders is important. And the converse of what Mr. Reed was just talking about is foreign governments' inability to access emails, communications, content, that happens to be U.S. held, even when they are investigating a local crime involving a local perpetrator and a local victim based on kind of out-moded rules from the 1980's Stored Communications Act.

As I said in my testimony, first the Obama administration, now again the Trump administration, have sent up legislation to the Hill that would begin to ease those restrictions. And I think it is something that Congress should take up to at least alleviate one of the pressures in favor of data localization.

Mr. GARFIELD. If I may, very quickly.

All of that is absolutely correct, but we are in an untenable position if the United States has to continually change its laws in order to respond to shifting court rules and dynamic in Europe. And so you asked about solutions. I think what is absolutely necessary here is American leadership in working with the rest of the world, not just Europe, to come up with rules of the road in this area. Because in the same way that the Privacy Shield can now be undermined by Schrems II, it will be Schrems III and IV a year from now.

Mr. WELCH. Yes.

Mr. GARFIELD. And so that is why our leadership in developing rules of the road in this area is so critically important.

Mr. WELCH. Thank you. I thank the panel.

Thank you, Mr. Chairman.

Mr. LATTA. Thank you very much. The gentleman's time has expired.

And the chair now recognizes the gentleman from Kentucky for 5—I am sorry. Mr. Lance is here. I am sorry. The gentleman from New Jersey for 5 minutes.

Mr. LANCE. Thank you very much. Kentucky is a great State, however, and very beautiful.

I want to thank the panel for joining us today to discuss this important topic.

The congressional district I serve is heavily involved in this field. Almost 60,000 constituents are employed in the high-tech sector. That is nearly 2 1A½ times greater than the average in a congressional district which, as I understand it, is 24,000. It is a driving force in our local economy and will continue to be as business and society become ever more reliant on advanced technologies.

Ms. Espinel, can you please explain how the free flow of data around the world supports emerging technology in machine learning and algorithms, for example, and the impact it has on businesses today?

Ms. ESPINEL. I would be happy to.

So machine learning is one aspect of artificial intelligence, and algorithms are the parameters or rules that let all kinds of artificial intelligence work. But artificial intelligence and the ability to be able to discern patterns and then help human beings make better decisions doesn't work in most circumstances unless you have fairly massive amounts of data. If you are a farmer looking at it trying to understand what is likely to happen in terms of weather conditions and, therefore, how you should be planting your fields and when you should be harvesting, if you are a manufacturer trying to understand what the consumer demand is around the world, if you are in cybersecurity and trying to track threats as they move across the world very rapidly, you can use artificial intelligence and data analytics to do a much, much better job of assessing what the outcomes will be in making decisions, but you can't unless you have large amounts of data to be able to do the data analytics and the artificial intelligence.

And in all of those areas I just mentioned, having international data is going to be very important. If you only have the ability to assess the weather patterns that are hanging right over the State of New Jersey or even just the United States, that is going to very much limit your ability to determine what is actually going to happen in terms of weather.

At the same time, if you are a manufacturer hoping to expand overseas and you can only get customer feedback from inside the United States, that is going to limit your ability to be able to best serve the largest amount of customers that you want to have. In cybersecurity, if you are limited to information that is in the United States, it will be virtually impossible to be able to detect patterns, because they move around the world so quickly.

So artificial intelligence depends on large amounts of data. But in many, many areas it also depends on having datasets that are coming from around the world with as little friction as possible in order to make them useful.

Mr. LANCE. Thank you very much.

Mr. Reed, are there any digital trade issues that are important to your members, small tech companies, that may be different from the priorities of larger companies?

Mr. REED. I think the issue of scale generally ends up being one of scarce resources. The reality is everyone here at this table has the same concerns when it comes to cross-border data flow. But let's consider it from a company in your district who has got, let's say, 20 employees. When they are looking at their CapEx expenditure, how much can they spend to build a data center or to source

something overseas? If they have got 20 employees, I have got to decide do I hire the 21st employee to deal with a contract I have for a company in New Jersey or do I try to spend that money to build a data center overseas?

So our primary issue that you are going to see the differentiation here is, for the larger companies, it is a cost but doable. For our folks, it becomes a barrier in which they cannot pass. And what becomes really disappointing about that outcome is, oftentimes, our companies are the one that drive forward the innovation. We get acquired by the big guys. We look forward to that opportunity to either beat them in the marketplace or get acquired and build another better product.

So the real differences that you are going to see in this space are where they say it is a cost, we say we can't go. And there is where we end up with the more significant painful and, frankly, anti-innovation damage that is done by trade barriers.

Mr. LANCE. Thank you.

Would anyone else on the panel like to comment?

Yes, Mr. Garfield.

Mr. GARFIELD. Well, I was going to give a concrete example. So we met with a company 2 weeks ago that is 4,000 people. And in order to comply with GDPR, they are putting 34 engineers against it. So GDPR is moving forward for legitimate reasons. But it speaks to the point that Mr. Reed made which is, for some companies, they can afford to assign 34 engineers. For others, they simply can't and so won't operate.

Mr. LANCE. Thank you. My time has expired.

Thank you, Mr. Chairman.

Mr. LATTA. Thank you very much. The gentleman yields back.

And now the chair recognizes the gentleman from Kentucky for 5 minutes.

Mr. GUTHRIE. Too bad he went first. He asked some of my questions, so I appreciate it very much.

But, no, it has actually been a fascinating panel, and you have all done such an excellent job. The things that I was going to ask you, really—I was going to talk about NAFTA. I wasn't going to say Mississippi. I was going to say Kentucky. But the same question that seems to be the same kind of answer, so I appreciate it.

I guess it is probably about 20 years now, but it was twin brothers who were in high school when they founded Hintcents, and they now have a very successful company, doing business in Bowling Green, so it is a great, great business.

I guess the one thing, there was a European Centre for International Political Economy that examined the consequences of GDP in countries that have cross-border restrictions, and under the sum of it is for safety and security, or there are a few of what is private. But in doing it for economics it says it decreases GDP in these countries that have these cross-border restrictions. So why would these countries do that?

Ms. ESPINEL. So I would certainly argue that it is not in the long-term economic interest of countries to put in data localization policies, although I can imagine that some may view it as being at least in their short-term economic interest because of a view that, if it is harder for U.S. companies to be operating inside of their bor-

ders, it will allow them to boost their domestic industry. I think longterm, that is not going to be the case. And I think it also is a real harm to their companies.

One of the things we have been talking about here, but I want to emphasize the point is, some of us are larger tech companies, some of us are smaller tech companies. What is really important here, I think, is the customers of our companies. And the customers of our companies are in every industry sector that exists. And that is true in the United States. That is true overseas as well.

So when governments put data localization policies in place, not only are they, in my view, hurting their own long-term economic interests in terms of building their tech industry, they are hurting the immediate economic interests of companies across their healthcare and manufacturing, transportation, other sectors, because they are denying them access to the latest innovation.

Mr. GARFIELD. The other thing is that businesses are so integrated today, both large and small, domestic and international; we represent companies all over the world. And they are codependent. And so when you put these rules in place, you do damage to your local businesses and customers.

Mr. GUTHRIE. We do a lot of stuff here when the States are doing, in the Commerce Clause, we have to kind of look at our role.

So I am going to go off the topic a minute; it is why you are here, Mr. Garfield. I met this morning with Secretary Acosta, Labor Secretary. Everywhere I go, people are talking about jobs, the right skills, the right skills for jobs. People are hiring, but people don't have the skills to move forward. And I am of a manufacturing background, so a lot of repetitive work has gone to automation. And some of your companies are involved in that, obviously. But as it goes to automation, the requirement to have somebody to be able to maintain that automation has raised, instead of being a \$14, \$15 person to the \$25, \$30, \$35 person an hour.

So your member companies are kind of driving this. What things are you guys doing—

Mr. GARFIELD. Yes.

Mr. GUTHRIE [continuing]. To help develop the workforce? And what can Congress do to help, is the question?

Mr. GARFIELD. It is completely on topic. I think one of the things you can do is what you are doing right now. So one of the examples you mentioned, I think banking, which is when ATMs came into the marketplace, most people assumed that there would be fewer people needed in banks. Well, the opposite is true. We have more ATMs around the world, but we have more people working in banks because there are more bank branches.

Part of the disconnect, there are 6 million open jobs in the country today and about 7 million people looking for work, that the challenge is that the skills of the people looking to work don't always match up with the jobs that exist. And so one of the things that we are putting a lot of energy behind, actually collectively, is making sure that we are reskilling the workforce such that those skills do align.

I think where Congress can help is by putting resources behind those efforts, but making sure that they are well coordinated so that there is closer connection between the private sector and the

public sector. The job training programs should be rooted in the needs of the world today, not the needs of the world 20 years ago.

Mr. GUTHRIE. Yes. It is also localized. I am on another committee that did the Workforce Investment and Innovation Act, WIOA, whatever they all stand for. And one of our main premises of changing it was make sure there was a business majority on the local boards and it is localized, because even though it is a global economy, there are certain things that happen in certain—people—they are clusters, and people become experts in their clusters.

Ms. ESPINEL. And if could just add to that briefly. I think the issue of reskilling and making sure that young people and people on their career paths have the skills that we need is a very important one, and I would echo everything that Dean just said. I think we also need to do a better job in terms of matching. So where people do have the skills and there is employee demand for those, making sure that the employees that have those needs are in touch with the people that have those skills. And I know there are training programs now that are being very intentional about making sure that, once you go through the training programs, there is also a clear path into a company that has a job. I think that is a very important part that we need to make sure is infused throughout our training programs to the extent possible.

I think this is a great area, though, for the industry, which is very focused on this and for Congress to be working together.

Mr. REED. I know we are out of time, but I think one of the issues that I want to differentiate a little bit from what we just discussed is, even though we are the software industry and we know what the salary is, I come from a background of working with machinery as well. And one of the things that is fascinating to me is not everybody needs to be a programmer. If you were in the manufacturing side of the world. Well, you know what a toolmaker is, you know what a patternmaker is. The same skill set that required you to be good with a file and good doing patternmaking, you transfer that same knowledge of a three-dimensional shape to a CAD program.

So when somebody says, well, I am a patternmaker, I don't know how to live in this precision manufacturing world, my sense is that is a failure on us, because the skill set, the idea, how does this fit together, where does this fit in the machinery, how do I make a better widget that goes better with this product, it is exactly the same as holding a file in one hand and a piece of metal in another or just putting the keyboard in between. And that, to a certain degree, is something we need to do to change the language about how we talk about reskilling and that we look at it from the standpoint of tools we are making to accomplish the same job are different, but the outcome is the same.

Mr. GUTHRIE. Thank you. My time has expired.

Mr. LATTA. Well, thank you very much.

And the chair now recognizes the gentlelady from California for 5 minutes.

Mrs. WALTERS. Thank you, Mr. Chairman.

Mr. Garfield, you state that data localization is the primary type of digital trade barrier. Can you describe which regions or coun-

tries have proposed or enacted nontariff measures like data localization or transfer of data restrictions?

Mr. GARFIELD. Yes, certainly. It is actually a long and growing list, unfortunately, so—there is a recent report from the Information Technology and Innovation Foundation that identifies 37 different countries. Their market is certainly like China, Indonesia, Vietnam, a number of South American markets that are now doing the same that is highly problematic. The thing that we have noted is that the motivations may be distinct in some of those markets. The drivers in Europe, for example, may be rooted in human rights and constitutional principles. But the end result is pernicious both for their local market and for global companies. And so there is a better approach to achieving the goals they have in mind.

Mrs. WALTERS. OK. Thanks. And have you recognized patterns in which certain regions or similarly situated countries justify nontariff measures based on a particular reasoning? For example, do you recognize that developing countries justify these barriers based on protectionism or whether geopolitical rivals to the U.S. justify their barriers on national security?

Mr. GARFIELD. I think the pattern that we see most often is that national security is the preeminent concern that is identified and articulated. The irony of it all is that national security is often undermined by localization requirements, because you are not getting patterns, as Victoria has pointed out or Mr. Reed has pointed out, from around the world. You are also closing yourself off from access to the best technologies that would actually support security.

And so part of this is addressing the legitimate security concerns while making sure they are not acting in a protectionist fashion.

Mrs. WALTERS. OK. The next question is for the entire panel. The testimony we have received for this hearing makes clear that the flow of data is really about the flow of ideas. Recently, some have advocated for the United States to implement a more protectionist trade policy. Are foreign countries reacting to this debate by moving toward additional policies to restrict data flows?

Ms. ESPINEL. Well, I will start because, actually, I think that is a nice follow-on from the question you just asked. And Dean talked about patterns. And I would agree that I think national security concerns is a pattern that we are seeing governments raise around the world. But another pattern that we are seeing is that governments that are not the United States are involved in trade or other bilateral discussions with governments around the world, and they are encouraging their vision of data or, in some cases, their lack of vision on data. And that is a troubling trend. And that is one of the reasons I think we and others have encouraged the United States to continue to show leadership on this issue.

The United States is using its trade negotiations, such as NAFTA, as sort of an immediate example or other bilateral discussions it is having to push for cross-border data flows. That is going to be very helpful in no small part because other governments are out saying that trade agreements or bilateral discussions either should not have rules on data flows or should have rules that would localize data. So I think that is an important aspect of this.

Mr. GARFIELD. It is not just theoretical, not to rehash TPP. But the Chinese model for data flows is almost 180 degree from ours.

But their influence in that region post-TPP is pronounced. I have spent a lot of time there in the last few months traveling between Japan, South Korea, and other markets in the region, and you can see the impact of that, particularly around data flows.

Ms. ESPINEL. And to give another example, the Japanese and the European Union are engaged in trade discussions right now. The Japanese are aligned with the United States, and they have been big promoters of cross-border data flows. Obviously, global innovation is a big part of their economy as well. But it looks like they are going to come to an agreement with the European Union that is going to leave this entire area out, rather than having rules on it as TPP and as we hope NAFTA would. So I think that is a troubling trend that we are seeing as well.

Mr. REED. And I will pile on. We just spent time dealing with Indonesia at, of all things, ITU, where there is an effort underway to essentially give the ITU power to control what is called over the top, which is essentially everything on the internet, through the ITU. And part of that is a move to restrict the success of the United States and the United States companies around data and get a lot of that under the control of the ITU and ultimately the United Nations.

I am sending staff around the world to deal with these exact issues from a small business perspective. So it is everywhere, it is pernicious. And ultimately, we are going to have to address it quickly.

Ms. DASKAL. And I would just add briefly, in addition to the protectionism concerns and the security motivating factors, there are, as we have talked about a little bit today, concerns about privacy, particularly amongst the EU. And there are steps that the United States can take both to take steps to improve its privacy protections both in the foreign intelligence surveillance regime and in the consumer privacy protection regime. And as Mr. Garfield said, also to play a leadership role in setting new norms and explaining better what the United States already does well.

Mr. REED. And I would be remiss if I didn't thank you for your current cosponsorship of H.R. 3718, which is legislation that helps to address some of that, the International Communications Privacy Act. So thank you.

Mrs. WALTERS. Thank you. And I am out of time. Thank you very much.

Mr. LATTA. Thank you. The gentlelady yields back.

The chair recognizes the gentleman from Florida for 5 minutes.

Mr. BILIRAKIS. Thank you very much. I appreciate it, Mr. Chairman. And I apologize for being late. We had a hearing and a markup in the VA Committee.

But I want to ask the question of Mr. Garfield. Each day, my constituents are utilizing internet-enabled tools to access customers abroad in ways impossible a decade ago, of course. American industries from manufacturing tools to financial services to agriculture are increasingly relying on the internet for their current and future global competitiveness, as you know. Unfortunately, U.S. internet services continue to face a number of market access and regulatory barriers.

As governments continue to assert a heavy hand on U.S. internet services, how would you use trade policies to stop other countries from blocking or discriminating against the U.S. services and ensure that the U.S. continues to lead the world in innovation?

Mr. GARFIELD. Thank you for the question. I would do what Congress suggested when it passed TPA, which is making sure that digital trade, trade promotion, cross-border data flows are a priority, and that we put in place mechanisms for holding markets accountable. It is not a theoretical issue. The United States is in the process of updating NAFTA and has said that they are on the path to do the same thing with the Korean trade agreement. I think in both instances we have the opportunity to ensure that all of the things that you identified that have an impact on the ground in Florida are, in fact, addressed.

Mr. BILIRAKIS. Thank you. Good answer. I appreciate that.

Mr. GARFIELD. I tried.

Mr. BILIRAKIS. Ms. Espinel. Is that how you pronounce it? Is that right?

Ms. ESPINEL. Espinel.

Mr. BILIRAKIS. OK. Thank you. I have a question for you. In your testimony, you explain how the services and technologies provided by your member companies are fundamentally affecting the ways in which companies are running their businesses, accessing markets, interacting with clients and customers, and generally innovating. How can trade agreements be used to help advance U.S. standards and best practices in protecting innovation and intellectual property like copyright, trade secrets, and, of course, patents?

Ms. ESPINEL. So one of the things that we have talked about a little bit today is the fact that, right now, one of the gaps in the international legal system is that there are no rules of the road. There is no international consensus on what data policy should be. And to me, it feels a little bit like where we were in the 1990s with intellectual property, investment, and services, where there were also no international rules of the road, or at least no trade international rules of the road. And at the time, the United States stepped up.

And as part of the negotiations that led to the establishment of the World Trade Organization, they said intellectual property, investment, services clearly—already important parts of the U.S. economy, clearly going to be even more important to the U.S. economy and the global economy. We need to have international trade rules. There need to be some internationally recognized parameters on how intellectual property, investment, and services should work cross border. And the U.S. pushed hard for that to happen. And I am very confident, without U.S. leadership, it would not have happened. But it did, and eventually, all of the members of the WTO countries agree that there should be international rules on intellectual property, investment, and services.

It feels to me like we are at that moment again for data. Data is also new. Although there has been so much progress and advance already, this is still a new industry. And the way it is impacting industry sectors across the economy is still relatively new. And that is part of the reason why there are no international rules on it yet.

And what I would ask Congress to do is to encourage the administration to look for places, NAFTA as an example, where we can start to set a precedent for international rules on data. I think it is clear that this is going to continue to be a very important part of the U.S. economy in the global economy, like IP investment and services. I am confident it is important so the economy will only grow over the next decade or so. And so we are going to need to have those rules. And I very much hope that this administration takes that mantle up and continues to work with countries around the world to try to set those rules.

As a former trade negotiator, that is not going to be easy discussion. That is not going to be a few days of discussions with other countries. It is a cutting edge issue, so it is going to be difficult. But it is so important, not just to our economy, but to the economy of our trading partners around the world. But I think it is very important.

And so whether it is NAFTA, whether it is Korea, whether it is discussions with the European Union and the U.K., whether it is discussions with Japan, whether it is discussions in multilateral venues, like the GS and the G8 and the G20, I would encourage the administration to be looking for every opportunity it can to start laying the ground rules for international trade rules on data.

Mr. BILIRAKIS. All right. Very good. Thank you very much.

I yield back, Mr. Chairman.

Mr. LATTA. The gentleman yields back.

And the chair recognizes the gentleman from Pennsylvania for 5 minutes.

Mr. COSTELLO. Thank you, Mr. Chairman.

As we all know, technological innovation shapes every State and region of the country. I am very proud in my southeastern Pennsylvania and congressional district, over 800 million high-tech manufacturing exports, over 200 million IT services exports, 42,000 high-tech sector workers, 30,000 STEM workers, over 17,000 computer and math workers, and over 12,000 highly educated immigrant workers.

My question, Mr. Garfield—and I appreciated your mention in your written testimony of several lead innovators from diverse industries and the many different ways they rely on cross-border data transmission as part of their core business function.

Merck, which employs several thousand just east of my district, but many live in my district, they have been able to deliver medical advancements more efficiently as the technology platforms they rely upon have grown increasingly global and sophisticated. I am asking you to elaborate on how removing barriers to cross-border data flows has the potential to increase business efficiency for medical innovators, create jobs, expedite the delivery of lifesaving therapies, and ultimately, lower costs for patient end users. In essence, how does removing these barriers translate into a higher quality of life both here and also in countries engaging in freer digital trade?

Mr. GARFIELD. Thank you. Thank you for the question. We were just noting that it makes me want to visit Pennsylvania just listening to your description of the place.

Mr. COSTELLO. Come on down.

Mr. GARFIELD. So the shortest answer to your question is that cross-border data flows allow us to look at patterns where we wouldn't know where to pull the information from. And so you would never know what insight you are going to get from these technologies which leads to greater innovation, greater collaboration, greater job creation, greater economic growth, and greater development in places like Pennsylvania.

And so the bottom line is cross-border data flows is really the oxygen, if you will, as I said at the beginning, for innovation today. And we all know the benefits of innovation and the broad-based impact that it has on economic development and growth in places like Pennsylvania, but throughout the country.

Mr. COSTELLO. Yes. And thank you for the answer—a couple other questions. But does anyone have anything to add different from that? Otherwise, I will move along.

OK. Next question. Have any studies been conducted on lost productivity that results from some of the current nontariff barriers to digital trade?

Ms. ESPINEL. I don't know one specifically. I know the U.S. Commerce Department has estimated that the digital trade is worth \$250 billion to the U.S. economy. But I am not familiar with the study that looks at lost productivity precisely.

That said, it is clear that cloud computing and data analytics and others contribute to productivity. So it is clear that it is going to have a negative significant impact. But I don't know of a specific study that has looked at that issue.

Mr. REED. I am happy to bring you some numbers on that. I think the way that we would look at that is the old what happens if you put your hand out and you spray paint around it? What we look for is countries nearby and regions nearby where they haven't seen the productivity growth that you should expect.

It is interesting you bring up Merck, because that is one of those where you can really see some impact on lifesaving drugs.

Mr. COSTELLO. I think the committee would certainly appreciate any feedback on that question further.

Mr. Garfield, data localization laws that contribute to the restriction of cross-border data flows. You mentioned the U.S. should work to establish new norms to remove some of those barriers. Two questions real quickly. Some of the nations you mentioned, have they demonstrated a willingness to help change the international norms? Second, besides formal negotiations, what else can be done to help change these international norms?

Mr. GARFIELD. The answer to the first is yes. So in Latin America, for example, we have seen some progress from private sector efforts to push countries away from the direction they were heading on restrictions on cross-border data flows. And so, yes, there is an opportunity there.

What more can you do? Or what can the U.S. do? I think, as we negotiate trade agreements, emphasizing the importance of digital trade and cross-border data flows and building in accountability mechanisms is a key part of that. My colleague tapped me on the shoulder to say that there is a report from ICIP and ITIF that gets into productivity, and we will make sure we get that report to you.

Mr. COSTELLO. Thank you.

I yield back. Thank you, Mr. Chairman.

Mr. LATTA. The gentleman yields back.

And seeing no other members seeking to ask questions, I would like to thank our witnesses today for appearing before us today.

And before we do conclude, I would like to include the following documents be submitted for the record by unanimous consent: a letter from Insights Association and a letter from Electronic Privacy Information Center.

[The information appears at the conclusion of the hearing.]

Mr. LATTA. Pursuant to committee rules, remind members that they have 10 business days to submit additional questions for the record. And I ask that the witnesses submit their responses within 10 business days upon receipt of the questions.

And, without objection, the subcommittee is adjourned.

[Whereupon, at 11:47 a.m., the subcommittee was adjourned.]

[Material submitted for inclusion in the record follows:]

#### PREPARED STATEMENT OF HON. FRANK PALLONE, JR.

Today's hearing is about the policies of foreign governments that affect the free flow of information across national boundaries. There is no dispute that the United States leads the world in technological innovation. And data continually crossing national borders is critical to that status.

Most of us don't spend much time thinking about how data is stored, how it moves, or how it affects our daily lives. But in our digital society, we rely on the ability of data to move quickly and seamlessly. It is essential to American innovation and enterprise.

Businesses of all types and sizes, and in virtually all industries, rely on data flows. For example, this near-instantaneous data flow happens when you use a credit card in another country to buy a sandwich or when you purchase a product from a company located overseas online. All sectors, including agriculture, mining, and manufacturing, are reliant on moving data.

The free flow of data allows business to flourish both domestically and abroad. Unnecessary barriers to these data flows affect the American economy and American jobs.

In recent years, a number of countries have begun to put policies in place that may hamper the free flow of information. Data localization policies take a number of forms, from explicit requirements that data be stored and processed within a country's borders to prohibitions on the transfer of personal information to countries that do not have adequate levels of data protection.

Governments assert a number of reasons for data localization policies. Concerns about law enforcement access to individuals' personal information have gotten a lot of attention in recent years following the disclosure of the NSA's surveillance programs.

Other factors are also at play—factors like competitiveness and antitrust concerns. In addition, national security and law enforcement interests have only increased in the wake of recent terror attacks all over the world. And some policies may be purely protectionist—to attempt to give local companies competitive advantage.

Like most Americans, citizens of other countries are troubled by the mass collection of personal information by private companies and whether that information is kept secure. Massive data breaches—like the Equifax breach, which affects British and Canadian citizens in addition to Americans—makes people even more nervous about their personal privacy. Enacting baseline consumer privacy and data security protections in this country can help ease those fears.

Meanwhile, addressing the other concerns of foreign citizens and foreign governments—those based on national security or economics—may require a combination of government and commercial actions to prevent harmful restrictions on cross border data flows.

I look forward to hearing from our witnesses on this important topic. Thank you.



October 10, 2017

**The Honorable Bob Latta**  
Chairman

**The Honorable Jan Schakowsky**  
Ranking Member

**Subcommittee on Digital Commerce and Consumer Protection**  
**House Energy & Commerce Committee**

**Subject: Hearing on 21st Century Trade Barriers on October 12**

Dear Chairman Latta and Ranking Member Schakowsky,

On behalf of the Insights Association,<sup>1</sup> the leading nonprofit trade association for the marketing research and analytics industry, thank you for holding this Thursday's hearing of the Digital Commerce and Consumer Protection Subcommittee on "21st Century Trade Barriers" and the vital issue of international digital trade.

Barriers to market access can take many forms, but restrictions on private sector cross-border data flows have become particularly burdensome: data localization laws, which require U.S. companies to physically store data in the country in which it originates; and laws like the European Union's (EU) General Data Protection Regulation (GDPR), which require U.S. companies to adopt significantly more restrictive foreign data privacy practices.

These laws and regulations have been enacted in many countries.<sup>2</sup> Often framed as concern about U.S. government surveillance, some are driven by foreign governments' desires to access their own citizens' data. However, even former President Obama called out the EU for using the GDPR as a pretext for digital protectionism.<sup>3</sup>

Local servers lead to a greater semblance of local control. They also generally require local workers, payment of local taxes, and submission to other local regulations. Meanwhile, "harmonization" of U.S. law to a foreign standard may not make the most sense economically, as innovative data businesses

<sup>1</sup> The Insights Association's membership includes both research and analytics companies and organizations, as well as the researchers and research departments inside of non-research companies and organizations. The Insights Association helps empower intelligent business decisions as a voice, resource, and network for the companies and individuals engaged in this important work.

<sup>2</sup> Testimony of Robert D. Atkinson, Information Technology and Innovation Foundation on "International Data Flows" at the House Subcommittee on Courts, Intellectual Property and the Internet. November 3, 2015. [http://www2.itif.org/2015-atkinson-international-data-flows.pdf?\\_ga=1.4629043.1886866732.1462063876](http://www2.itif.org/2015-atkinson-international-data-flows.pdf?_ga=1.4629043.1886866732.1462063876)

<sup>3</sup> President Barack Obama: "Sometimes the European response here is more commercially driven than anything else. ...sometimes their vendors — their service providers who, you know, can't compete with ours — are essentially trying to set up some roadblocks for our companies to operate effectively there." <http://www.marketingresearch.org/article/obama-calls-out-european-data-protection-plain-protectionism>

INSIGHTS ASSOCIATION

1156 15TH ST, NW, SUITE 302, WASHINGTON, DC 20005 • PH: (202) 570-7312

WEBSITE: [www.InsightsAssociation.org](http://www.InsightsAssociation.org) • EMAIL: [howard.fienberg@insightsassociation.org](mailto:howard.fienberg@insightsassociation.org)

generally develop and grow in the U.S., and our approach to data privacy may be a key factor in our competitive advantage.<sup>4</sup>

Although the Insights Association was disappointed by the U.S. abandonment of the Trans Pacific Partnership (TPP) trade agreement, because of the important provisions to facilitate cross-border data flows, but we have appreciated the Trump Administration's focus on similar principles in the current renegotiation of the North American Free Trade Agreement (NAFTA), including: the establishment of rules to prevent "measures that restrict crossborder data flows" or "require the use or installation of local computing facilities"; getting signatories agreement "not to impose customs duties on digital products" (like research and analytics software); and demanding "non-discriminatory treatment of digital products transmitted electronically" and "fair and open conditions for services trade."

We also encourage the Subcommittee to examine the complicated challenges facing U.S.-EU digital trade. We rolled with the punches when the European Union Court of Justice struck down the Safe Harbor, encouraging our members to embrace its replacement arrangement, the U.S.-EU Privacy Shield. However, the Irish Data Protection Commissioner just referred the underlying case, Schrems v. Facebook, back to the EU high court again, based on concerns about the data protection "adequacy" of model clauses as a mechanism for data transfers to the U.S. The challenge could potentially lead to the court striking down not just the model clauses, relied upon by many companies, but the newly-vital Privacy Shield agreement as well, endangering most every trans-Atlantic data transfer.

The Insights Association looks forward to your October 12 hearing, and working with the Subcommittee to support the ability of American businesses to share data across borders, in furtherance of domestic economic growth.

Sincerely,



Howard Fienberg  
Director of Government Affairs  
Insights Association

<sup>4</sup> "Corporate privacy officers discuss global compliance, trans-Atlantic competition, a comprehensive privacy law, and the US-EU Safe Harbor." March 7, 2013. <http://www.marketingresearch.org/article/corporate-privacy-officers-discuss-global-compliance-trans-atlantic-competition>

**epic.org**

**Electronic Privacy Information Center**  
1718 Connecticut Avenue NW, Suite 200  
Washington, DC 20009, USA

+1 202 483 1140  
+1 202 483 1248  
@EPICPrivacy  
<https://epic.org>

October 11, 2017

The Honorable Robert Latta, Chairman  
The Honorable Janice Schakowsky, Ranking Member  
U.S. House Committee on Energy and Commerce  
Subcommittee on Digital Commerce & Consumer Protection  
2125 Rayburn House Office Building  
Washington, D.C. 20515

Dear Chairman Latta and Ranking Member Schakowsky:

We write to you regarding the “21st Century Trade Barriers: Protectionist Cross Border Data Flow Policy’s Impact on U.S. Jobs” hearing.<sup>1</sup> We appreciate the Committee’s interest in this important topic, but hope that you will consider the urgent need to update privacy laws in the United States as you examine the reasons that foreign governments may be reluctant to permit the transfer of personal data.

EPIC is a public interest research center established in 1994 to focus public attention on emerging privacy and civil liberties issues.<sup>2</sup> EPIC has previously testified before this Committee on this issue and has made recommendations on how the US and Europe could move forward to address shared concerns about the protection of privacy.<sup>3</sup> Those recommendations have gained greater force over time.

American consumers today face unprecedented privacy threats and security risks. The unregulated collection of personal data has led to staggering increases in identity theft, security

<sup>1</sup> *21st Century Trade Barriers: Protectionist Cross Border Data Flow Policy’s Impact on U.S. Jobs*, 115<sup>th</sup> Cong. (2017), H. Comm. on Energy & Commerce, Subcomm. on Digital Commerce and Consumer Protection, <https://energycommerce.house.gov/hearings/21st-century-trade-barriers-protectionist-cross-border-data-flow-policies-impact-u-s-jobs/> (Oct. 12, 2017).

<sup>2</sup> See EPIC, *About EPIC*, <https://epic.org/epic/about.html>.

<sup>3</sup> Marc Rotenberg, EPIC Executive Director, Testimony before the House Comm. on Energy & Commerce, Subcomm. on Communications and Technology, *Examining the EU Safe Harbor Decision and Impacts for Transatlantic Data Flows* (November 13, 2015), <https://epic.org/privacy/intl/schrems/EPIC-EU-SH-Testimony-HCEC-11-3-final.pdf>; Marc Rotenberg, “They’re Right to Distrust U.S. Data Security”, *Wall Street Journal* (March 22, 2016); Marc Rotenberg, “Digital Privacy, in US and Europe,” *N.Y. Times*, Oct. 13, 2015; Marc Rotenberg, “On International Privacy: A Path Forward for the US and Europe,” *Harvard International Review* (Spring 2014); Marc Rotenberg & David Jacobs, “Updating the Law of Information Privacy: The New Framework of the European Union,” *Harvard Journal of Law and Public Policy* (Spring 2013); Marc Rotenberg, “Better Privacy Laws: Priority for America and Germany,” *N.Y. Times*, Sept. 3, 2013.

breaches, and financial fraud in the United States.<sup>4</sup> The Equifax data breach revealed last month that exposed the personal information of approximately 145.5 million Americans<sup>5</sup> is the latest in a growing number of high-profile hacks that threaten the privacy, security, and financial stability of American consumers. Far too many organizations collect, use, and disclose detailed personal information with too little regard for the consequences.

The United States should take four steps to update domestic privacy law: (1) enact the Consumer Privacy Bill of Rights, (2) modernize the Privacy Act, (3) establish an independent data protection agency, and (4) ratify the International Privacy Convention. This is the strategy that enables cross border data flows to continue and protects the interests of US consumers and US businesses.

### **The Federal Trade Commission Has Failed to Pursue Meaningful Enforcement**

The FTC is simply not doing enough to safeguard the personal data of American consumers. While we respect the efforts of the Commission to protect consumers, the reality is that the FTC lacks the statutory authority, the resources, and the political will to adequately protect the online privacy of American consumers.

The FTC's privacy framework – based largely on “notice and choice” – is simply not working. Research shows that consumers rarely read privacy policies; when they do, these complex legal documents are difficult to understand. Nor can industry self-regulatory programs provide realistic privacy protections when they are not supported by enforceable legal standards.

Even when the FTC reaches a consent agreement with a privacy-violating company, the Commission rarely enforces the Consent Order terms.<sup>6</sup> American consumers whose privacy has been violated by unfair or deceptive trade practices do not have a private right of action to obtain redress. Only enforceable privacy protections create meaningful safeguards, and the lack of FTC enforcement has left consumers with little recourse.

Last month, the FTC announced a settlement with three companies that misrepresented their participation in the Privacy Shield arrangement.<sup>7</sup> The Privacy Shield<sup>8</sup> allows companies to transfer the personal data of European consumers to the United States based on a system of industry self-certification. The FTC settlement prohibits the companies from making future false claims about compliance with Privacy Shield, but does not impose any penalty. The FTC settlement also fails to provide any remedy to the EU consumers whose personal data was

<sup>4</sup> Fed. Trade Comm'n, *Consumer Sentinel Network Data Book* (Feb. 2016), <https://www.ftc.gov/system/files/documents/reports/consumer-sentinel-network-data-book-january-december-2015/160229csn-2015databook.pdf>.

<sup>5</sup> Equifax, *Cybersecurity Incident & Important Consumer Information*, <https://www.equifaxsecurity2017.com/frequently-asked-questions/>.

<sup>6</sup> See *EPIC v. FTC*, No. 12-206 (D.C. Cir. Feb. 8, 2012).

<sup>7</sup> Press Release, Federal Trade Comm'n, Three Companies Agree to Settle FTC Charges They Falsely Claimed Participation in EU-US Privacy Shield Framework (Sept. 8, 2017), <https://www.ftc.gov/news-events/press-releases/2017/09/three-companies-agree-settle-ftc-charges-they-falsely-claimed>.

<sup>8</sup> EPIC, *Privacy Shield EU-U.S. Data Transfer Arrangement*, <https://epic.org/privacy/intl/privacy-shield/>.

wrongfully obtained, nor does it require the companies to disgorge the data they fraudulently obtained.

#### **Privacy Shield Is Not an Effective Basis for EU-US Data Flows**

EPIC and many others are concerned about the adequacy of the Privacy Shield and the protection of consumer data.<sup>9</sup> Without more substantial reforms to ensure protection for fundamental rights of individuals on both sides of the Atlantic, the Privacy Shield will put users at risk and undermine trust in the digital economy. Specifically, the United States must commit to protecting the data privacy of both US-persons and non-US-persons in order to protect users and instill trust in the digital economy.<sup>10</sup>

Neither consumers nor businesses want to see the disruption of cross border data flows. But the problems of inadequate data protection in the United States can no longer be ignored. US consumers are suffering from skyrocketing problems of identity theft, data breach, and financial fraud. Not surprisingly, European governments are very concerned about what happens to the personal information of their citizens when it is transferred to the United States. Privacy Shield does not solve this problem. The US will need to do more to reform privacy law to enable cross border data flows. It is a well-known paradox that promoting the free flow of personal data across national boundaries requires comprehensive privacy protection.<sup>11</sup>

#### **The Schrems II Decision Could Have Far-reaching Consequences if the US Fails to Act**

The Irish High Court's decision<sup>12</sup> released last week calls into question the viability of the current data transfer scheme between the US and EU. As a general principle, EU law prohibits data transfers outside of the EU where strict EU privacy laws do not apply, but there are exceptions. One exception was Safe Harbor, but two years ago, the Court of the Justice of the European Union invalidated it.<sup>13</sup> This case originated from a complaint brought by Max Schrems against Facebook Ireland Ltd. before the Irish Data Protection Commissioner in 2013. After it could no longer use Safe Harbor, Facebook used another legal mechanism—Standard Contractual Clauses (also known as Model Clauses)—to facilitate data transfers to the US. Standard Contractual Clauses are contracts between European and American companies whereby American companies agree to abide by European privacy law. The Irish Data Protection Commissioner has taken the position that Standard Contractual Clauses are invalid under EU

<sup>9</sup> See, e.g., Testimony of Marc Rotenberg, EPIC Executive Director, Testimony before the U.S. House of Representatives Energy & Commerce Subcommittees on Commerce, Manufacturing, and Trade and Communications and Technology, *Examining the EU Safe Harbor Decision and Impacts for Transatlantic Data Flows* (Nov. 3, 2015), <https://epic.org/privacy/intl/schrems/EPIC-EU-SH-Testimony-HCEC-11-3-final.pdf>.

<sup>10</sup> See, e.g., Letter from EPIC, et al., to Article 29 Working Party Chairman Isabelle Falque-Pierrotin, et al., on Privacy Shield (Mar. 16, 2016), <https://epic.org/privacy/intl/schrems/Priv-Shield-Coalition-LtrMar2016.pdf>.

<sup>11</sup> Marc Rotenberg, On International Privacy: A Path Forward for the US and Europe, Harvard International Review (June 15, 2014), <http://hir.harvard.edu/on-international-privacy-a-path-forward-for-the-us-and-europe/>.

<sup>12</sup> Data Protection Commissioner v. Facebook Ireland Limited and Maximilian Schrems [2017] (Ir.).

<sup>13</sup> Maximilian Schrems v. Data Protection Commissioner [2015] (E.C.J.).

law, referred the case to the Court of the Justice of the European Union to resolve this question. Once again, the highest European court will have the opportunity to invalidate a mechanism commonly used to facilitate transfers between American and European companies.

This case highlights the urgency of the need for the US to take action to protect user privacy. The United States should not update its privacy law because of a judgment of the European Court. The United States should update its privacy law because it is long overdue, because it is widely supported, and because the ongoing failure to modernize privacy law is imposing enormous costs on American consumers.

#### **To Support Cross Border Data Flows, Congress Must Modernize US Privacy Law**

There are at least four steps that Congress needs to take to address concerns about data protection in the United States. This is the strategy that enables cross border data flows to continue and protects the interests of US consumers and US businesses.

First, Congress should enact the Consumer Privacy Bill of Rights. The Consumer Privacy Bill of Rights is a sensible framework that would help establish fairness and accountability for the collection and use of personal information. It is based on familiar principles for privacy protection that are found in many laws in the United States. This framework would establish baseline safeguards for the development of innovative services that take advantage of technology while safeguarding privacy. But the key to progress is the enactment by Congress. Only enforceable privacy protections create meaningful safeguards.

Second, Congress should modernize the Privacy Act, revise the scope of the Act's coverage and clarify the damages provision. There are many changes that need to be made to the law to protect the interests of Americans. The Judicial Redress Act does not provide adequate protection to permit data transfers and it does not address the many provisions in the Privacy Act that need to be updated.<sup>14</sup>

Third, Congress should create an independent privacy agency, as Congress contemplated in 1974 when it enacted the Privacy Act.<sup>15</sup> EPIC has previously recommended the establishment of a privacy agency to ensure independent enforcement of the Privacy Act, develop additional recommendations for privacy protection, and provide permanent leadership within the federal government on this important issue.<sup>16</sup> This independent privacy agency would be charged with enforcing privacy laws. Enforcement should not be assigned to the FTC, as the FTC has missed many opportunities to strengthen US privacy law.

<sup>14</sup> See generally, EPIC, EU-US Data Transfer Agreement (2015), <https://epic.org/privacy/intl/data-agreement/index.html>.

<sup>15</sup> Staff of S. Comm. on Gov't Operations, 93d Cong., Materials Pertaining to S. 3418 and Protecting Individual Privacy in Federal Gathering, Use and Disclosure of Information (Comm. Print 1974) (collecting materials on S. 3418, a bill to establish a Federal Privacy Board).

<sup>16</sup> See, e.g., Marc Rotenberg, *In Support of a Data Protection Board in the United States*, 8 Gov't Info. Q. 79 (1991); *Communications Privacy: Hearing Before the Subcomm. on Courts and Intellectual Prop. of H. Comm. on the Judiciary*, 105th Cong. (1998) (testimony of Marc Rotenberg), available at <https://www.epic.org/privacy/internet/rotenberg-testimony-398.html>.

Fourth, the final step to address the growing EU-US divide is to ratify the international Privacy Convention 108, the most-well established legal framework for international data flows.<sup>17</sup> The Privacy Convention would establish a global bias to safeguard personal information and enable the continued growth of the Internet economy. In the absence of a formal legal agreement, it is likely that other challenges to self-regulatory frameworks will be brought.

This is not simply a matter of trade policy. It is a matter of fundamental rights. There is today a growing consensus on both sides of the Atlantic, supported by consumer groups and business leaders, to recognize that privacy is a fundamental human right.

As a general proposition, we support the free flow of information and oppose protectionist barriers. But the failure of the United States to ensure meaningful privacy protection for personal data is the reason that a growing number of countries are concerned about trans-border data flows. Until that problem is addressed, concerns about data transfers to the United States will remain.

We ask that this Statement from EPIC be entered in the hearing record. We look forward to working with you on these issues of vital importance to the American public.

Sincerely,

/s/ Marc Rotenberg  
Marc Rotenberg  
EPIC President

/s/ Caitriona Fitzgerald  
Caitriona Fitzgerald  
EPIC Policy Director

/s/ Christine Bannan  
Christine Bannan  
EPIC Policy Fellow

---

<sup>17</sup> See generally, EPIC, Council of Europe Privacy Convention (2015), <https://epic.org/privacy/intl/coeconvention/>.

GREG WALDEN, OREGON  
CHAIRMAN

FRANK PALLONE, JR., NEW JERSEY  
RANKING MEMBER

ONE HUNDRED FIFTEENTH CONGRESS  
**Congress of the United States**  
**House of Representatives**  
COMMITTEE ON ENERGY AND COMMERCE  
2125 RAYBURN HOUSE OFFICE BUILDING  
WASHINGTON, DC 20515-6115  
Majority (202) 225-2927  
Minority (202) 225-3641  
October 27, 2017

Ms. Victoria A. Espinel  
President and CEO  
BSA - The Software Alliance  
20 F Street, N.W.  
Washington, DC 20001

Dear Ms. Espinel:

Thank you for appearing before the Subcommittee on Digital Commerce and Consumer Protection on Thursday, October 12, 2017, to testify at the hearing entitled "21st Century Trade Barriers: Protectionist Cross Border Data Flow Policies' Impact on U.S. Jobs."

Pursuant to the Rules of the Committee on Energy and Commerce, the hearing record remains open for ten business days to permit Members to submit additional questions for the record, which are attached. The format of your responses to these questions should be as follows: (1) the name of the Member whose question you are addressing, (2) the complete text of the question you are addressing in bold, and (3) your answer to that question in plain text.

To facilitate the printing of the hearing record, please respond to these questions by the close of business on Monday, November 13, 2017. Your responses should be mailed to Ali Fulling, Legislative Clerk, Committee on Energy and Commerce, 2125 Rayburn House Office Building, Washington, DC 20515 and e-mailed in Word format to [ali.fulling@mail.house.gov](mailto:ali.fulling@mail.house.gov).

Thank you again for your time and effort preparing and delivering testimony before the Subcommittee.

Sincerely,



Robert E. Latta  
Chairman  
Subcommittee on Digital Commerce  
and Consumer Protection

cc: Jan Schakowsky, Ranking Member, Subcommittee on Digital Commerce and Consumer Protection

Attachment

Additional Question for the Record – Victoria Espinel

**The Honorable Michael C. Burgess**

**Question:** How can differing notions of data privacy be addressed particularly between two or more countries that have fundamentally different understandings of what constitutes “sufficient” privacy of personal data?

**Answer:** Although countries around the world have implemented different privacy frameworks, many of the underlying principles—such as protecting the security of personal information or increasing transparency of data handling practices—are the same.

As we seek to facilitate digital trade to spur innovation and global economic growth, countries must work together to leverage the commonalities underpinning their privacy frameworks and find ways to bridge the differences.

There are important examples of existing efforts to enhance interoperability among different privacy systems. The EU-U.S. Privacy Shield Framework provides a critical mechanism that both protects individual privacy and facilitates transatlantic trade. In the Asia-Pacific region, the APEC Cross-Border Privacy Rules implement a robust system that establishes baseline privacy practices and promotes trade among participating economies, all while respecting national privacy laws.

As countries continue to adopt, revise, and implement privacy laws, they should develop policy approaches that enhance global interoperability. The development of pragmatic solutions that not only provide important privacy protections, but also enable global data flows across countries with different national systems is critical for digital trade to flourish.

GREG WALDEN, OREGON  
CHAIRMAN

FRANK PALLONE, JR., NEW JERSEY  
RANKING MEMBER

ONE HUNDRED FIFTEENTH CONGRESS  
**Congress of the United States**  
**House of Representatives**  
COMMITTEE ON ENERGY AND COMMERCE  
2125 RAYBURN HOUSE OFFICE BUILDING  
WASHINGTON, DC 20515-6115  
Majority (202) 225-2927  
Minority (202) 225-3641  
October 27, 2017

Mr. Dean C. Garfield  
President and CEO  
Information Technology Industry Council  
1101 K Street, N.W., Suite 610  
Washington, DC 20005

Dear Mr. Garfield:

Thank you for appearing before the Subcommittee on Digital Commerce and Consumer Protection on Thursday, October 12, 2017, to testify at the hearing entitled "21st Century Trade Barriers: Protectionist Cross Border Data Flow Policies' Impact on U.S. Jobs."

Pursuant to the Rules of the Committee on Energy and Commerce, the hearing record remains open for ten business days to permit Members to submit additional questions for the record, which are attached. The format of your responses to these questions should be as follows: (1) the name of the Member whose question you are addressing, (2) the complete text of the question you are addressing in bold, and (3) your answer to that question in plain text.

To facilitate the printing of the hearing record, please respond to these questions by the close of business on Monday, November 13, 2017. Your responses should be mailed to Ali Fulling, Legislative Clerk, Committee on Energy and Commerce, 2125 Rayburn House Office Building, Washington, DC 20515 and e-mailed in Word format to [ali.fulling@mail.house.gov](mailto:ali.fulling@mail.house.gov).

Thank you again for your time and effort preparing and delivering testimony before the Subcommittee.

Sincerely,



Robert E. Latta  
Chairman  
Subcommittee on Digital Commerce  
and Consumer Protection

cc: Jan Schakowsky, Ranking Member, Subcommittee on Digital Commerce and Consumer Protection

Attachment



November 9, 2017

The Honorable Bob Latta  
Chairman, Subcommittee on Digital Commerce and Consumer Protection  
Committee on Energy & Commerce  
2125 Rayburn House Office Building  
Washington, D.C. 20515

RE: Question for the Record  
Hearing on "21<sup>st</sup> Century Trade Barriers: Protectionist Cross Border Data Flow Policies' Impact on U.S. Jobs"

Dear Chairman Latta:

Thank you again for the opportunity to testify before the Subcommittee on October 12, 2017, on the importance of digital trade to U.S. jobs and the economy. Enclosed you will find my response to the question for the record submitted to me by Dr. Burgess.

As the Subcommittee continues its work and oversight on this matter, please consider me as a resource.

Sincerely,

A handwritten signature in black ink, appearing to read "Dean C. Garfield", written in a cursive style.

Dean C. Garfield  
President & CEO



The Honorable Michael C. Burgess

1. In your testimony you note that enabling cross-border data flows and curbing data localization are important to the success of multinational technology companies like the ones in your association. In what ways do these policies impact the health care and public health sector?

In my testimony I explained how all industries – from manufacturing to agriculture – rely on cross-border data flows to remain competitive in the global economy, and the health sector is no different. The free flow of data allows health care professionals to collaborate overseas to run tests and find cures to diseases. It allows new, cutting-edge treatments to be disseminated among hospitals and local doctors and reach patients at never before realized rates, regardless of their country of origin. It helps public health officials respond to and treat public health outbreaks across oceans before diseases can be spread to new areas. The health sector, perhaps more than many others, has been transformed by the internet and the free flow of data across borders.

However, concerns about the security of that data and protecting the privacy of patients must be addressed in order to fully realize these benefits and build trust between doctors, patients, companies, and governments. Some countries, such as China and Australia, have opted to force companies to keep patient data within the borders of their countries – this is a mistake. Measures of this type degrade the ability of doctors, academics, and health professionals to collaborate and share information to bring state-of-the-art treatment to their markets. Additionally, as I explained in my testimony, restricting the ability of companies to transfer information over border raises the cost for companies to host and process data. In the health sector, what this translates to is increased healthcare costs and a degradation of the ability of American technology companies and health companies to do business in those markets.

Concerns about security and privacy, of course, are legitimate and worth considering. First, it is important to understand that data security is not a function of its location. Security is the result of companies and governments using best security practices across their networks and technologies. For responsible handlers of data, this is built into their systems and cultures, regardless of location of data facilities. In fact, requiring specifically health data to be stored within certain borders can make it less secure because bad actors will know exactly which systems need to be breached to obtain access to that data.

In addition, medical data privacy can be achieved without incurring the economic costs and discriminatory nature of forced data localization. Governments absolutely should protect the privacy of their citizens, but this can be done with interoperable, globally oriented privacy regimes. I believe that the Cross-Border Privacy Rules (CBPR) created under the auspices of the Asia-Pacific Economic Cooperation Forum (APEC) is a good example of such an international program. Under this system, companies and government certify to a set of privacy standards to which data must be handled in order to be transferred between countries. Countries can also set sector-specific standards for particularly sensitive data, such as medical data, to further ensure that their citizens are adequately protected when it is being transferred overseas.

I hope that this thoroughly answers your question, and I am happy to expand further if you have any additional follow-up. Thank you.

GREG WALDEN, OREGON  
CHAIRMAN

FRANK PALLONE, JR., NEW JERSEY  
RANKING MEMBER

ONE HUNDRED FIFTEENTH CONGRESS  
**Congress of the United States**  
**House of Representatives**  
COMMITTEE ON ENERGY AND COMMERCE  
2125 RAYBURN HOUSE OFFICE BUILDING  
WASHINGTON, DC 20515-6115  
Majority (202) 225-2927  
Minority (202) 225-3641  
October 27, 2017

Mr. Morgan Reed  
President  
ACT - The App Association  
1401 K Street, N.W., Suite 501  
Washington, DC 20005

Dear Mr. Reed:

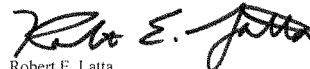
Thank you for appearing before the Subcommittee on Digital Commerce and Consumer Protection on Thursday, October 12, 2017, to testify at the hearing entitled "21st Century Trade Barriers: Protectionist Cross Border Data Flow Policies' Impact on U.S. Jobs."

Pursuant to the Rules of the Committee on Energy and Commerce, the hearing record remains open for ten business days to permit Members to submit additional questions for the record, which are attached. The format of your responses to these questions should be as follows: (1) the name of the Member whose question you are addressing, (2) the complete text of the question you are addressing in bold, and (3) your answer to that question in plain text.

To facilitate the printing of the hearing record, please respond to these questions by the close of business on Monday, November 13, 2017. Your responses should be mailed to Ali Fulling, Legislative Clerk, Committee on Energy and Commerce, 2125 Rayburn House Office Building, Washington, DC 20515 and e-mailed in Word format to [ali.fulling@mail.house.gov](mailto:ali.fulling@mail.house.gov).

Thank you again for your time and effort preparing and delivering testimony before the Subcommittee.

Sincerely,



Robert E. Latta  
Chairman  
Subcommittee on Digital Commerce  
and Consumer Protection

cc: Jan Schakowsky, Ranking Member, Subcommittee on Digital Commerce and Consumer Protection

Attachment

The Honorable Michael C. Burgess

***Is there a critical role that Congress can play in this discussion? What do you think are the top two ways in which this Committee and Congress can address barriers to digital trade for small tech companies like your members?***

Yes, Congress can play a critical role in the digital trade space. First, Congress—and the Subcommittee on Digital Commerce and Consumer Protection in particular—should exercise its oversight authority and empower trade negotiators in their efforts to ensure the free flow of data across national borders to give American innovators, particularly small and medium-sized enterprises (SMEs), opportunities to grow their customer bases and create more American jobs. For example, the negotiating objectives set forth by the United States Trade Representative (USTR) for the North American Free Trade Agreement (NAFTA) seek to “establish rules to ensure that NAFTA countries do not impose measures that restrict cross-border data flows . . .” ACT | The App Association strongly supports this negotiating objective. But as the negotiation over the trade agreement progresses, some of our most important priorities could be sacrificed for others without congressional input.

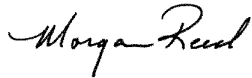
As the former chairman of the Subcommittee, we appreciate your efforts to position the Subcommittee as a leader on digital trade issues. Your work in highlighting the trade barriers that prevent cross-border data flows is vitally important and helps ensure that our negotiators understand that such safeguards should remain part of NAFTA and future trade agreements. The International Trade Commission (ITC) estimates that U.S. GDP increased significantly (between 3.4 percent and 4.8 percent) in 2011 as a result of digital trade. That year, ITC estimated that digital trade helped create 2.4 million jobs in the United States,<sup>1</sup> and the role of cross-border data flows in today’s economy has only expanded. The growth that the digital economy drives depends heavily on the ability for U.S. companies, particularly SMEs, to easily access new markets seamlessly transferring data across political borders. This need must be a top trade negotiation priority in NAFTA and other negotiations, but is potentially jeopardized when our trade negotiators must focus on so many other aspects of the economy. Therefore, as part of these efforts, the Subcommittee has, and should continue to, lead Congress in providing a forum for experts, industry, and policymakers to publicly discuss, craft, and promote a single U.S. position on digital trade that maintains cross-border data flows as a top priority (along with other key digital trade priorities I detailed in my written and oral testimony) through further hearings and oversight activity. This activity would help by a) reinforcing the importance of digital trade to Congress and other stakeholders; and b) cementing the Subcommittee’s role as an expert body and leading policymaker in the digital trade debate.

Second, it is imperative that Congress provide as much legal certainty as possible to U.S. businesses seeking to leverage the growing digital economy to expand their businesses and create new American jobs, particularly the SMEs that do not have the resources that large corporations may have to account for such uncertainties. As a leading example, the App Association calls on Congress to resolve threshold liability questions related to warrants and data stored abroad by passing the International Communications Privacy Act (ICPA, H.R. 3718) as soon as practicable. ICPA would clarify when and how U.S. law enforcement agencies may access data pertaining to foreign persons stored by U.S. communications providers overseas. As the law in this area is

<sup>1</sup> <http://www.usitc.gov/publications/332/pub4485.pdf>.

unclear and unlikely to be fully clarified by a pending case at the U.S. Supreme Court (*United States v. Microsoft*), ICPA's passage is timely and needed. Enacting ICPA, or legislation like it, would reduce crippling legal uncertainty for our member companies and other American businesses looking to access overseas markets. It would also provide cover to American trade negotiators as they seek to show foreign governments that our privacy protections are equal to theirs. It is unfortunately common for policies that interrupt data transfers to be based, at least in part, on a mistrust of U.S. approaches to data privacy. More must be done to ensure that companies conducting business abroad do not face conflicts between law enforcement requests and foreign laws. We believe that ICPA would ameliorate these conflicts between foreign laws and U.S. law enforcement agencies' authority to obtain data pertaining to foreign citizens, which would in turn remove a trade barrier. Further, ICPA would ensure that the United States continues to lead other nations in providing for rule of law and due process.

Sincerely,

A handwritten signature in black ink that reads "Morgan Reed". The signature is fluid and cursive, with the first name "Morgan" and last name "Reed" clearly distinguishable.

Morgan Reed  
President  
ACT | The App Association