AUTHENTICATED
U.S. GOVERNMENT
INFORMATION
GPO

CROSS-BORDER DATA FLOWS: COULD FOREIGN PROTECTIONISM HURT U.S. JOBS?

HEARING

BEFORE THE

SUBCOMMITTEE ON COMMERCE, MANUFACTURING, AND TRADE

OF THE

COMMITTEE ON ENERGY AND COMMERCE

HOUSE OF REPRESENTATIVES

ONE HUNDRED THIRTEENTH CONGRESS

SECOND SESSION

SEPTEMBER 17, 2014

Serial No. 113–176



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

U.S. GOVERNMENT PUBLISHING OFFICE

95–852 PDF WASHINGTON : 2015

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

FRED UPTON, Michigan
Chairman

RALPH M. HALL, Texas
JOE BARTON, Texas
Chairman Emeritus
ED WHITFIELD, Kentucky
JOHN SHIMKUS, Illinois
JOSEPH R. PITTS, Pennsylvania
GREG WALDEN, Oregon
LEE TERRY, Nebraska
MIKE ROGERS, Michigan
TIM MURPHY, Pennsylvania
MICHAEL C. BURGESS, Texas
MARSHA BLACKBURN, Tennessee
Vice Chairman
PHIL GINGREY, Georgia
STEVE SCALISE, Louisiana
ROBERT E. LATTA, Ohio
CATHY MCMORRIS RODGERS, Washington
GREGG HARPER, Mississippi
LEONARD LANCE, New Jersey
BILL CASSIDY, Louisiana
BRETT GUTHRIE, Kentucky
PETE OLSON, Texas
DAVID B. MCKINLEY, West Virginia
CORY GARDNER, Colorado
MIKE POMPEO, Kansas
ADAM KINZINGER, Illinois
H. MORGAN GRIFFITH, Virginia
GUS M. BILIRAKIS, Florida
BILL JOHNSON, Ohio
BILLY LONG, Missouri
RENEE L. ELLMERS, North Carolina

HENRY A. WAXMAN, California
Ranking Member
JOHN D. DINGELL, Michigan
FRANK PALLONE, JR., New Jersey
BOBBY L. RUSH, Illinois
ANNA G. ESHOO, California
ELIOT L. ENGEL, New York
GENE GREEN, Texas
DIANA DEGETTE, Colorado
LOIS CAPPS, California
MICHAEL F. DOYLE, Pennsylvania
JANICE D. SCHAKOWSKY, Illinois
JIM MATHESON, Utah
G.K. BUTTERFIELD, North Carolina
JOHN BARROW, Georgia
DORIS O. MATSUI, California
DONNA M. CHRISTENSEN, Virgin Islands
KATHY CASTOR, Florida
JOHN P. SARBANES, Maryland
JERRY MCNERNEY, California
BRUCE L. BRALEY, Iowa
PETER WELCH, Vermont
BEN RAY LUJAN, New Mexico
PAUL TONKO, New York
JOHN A. YARMUTH, Kentucky

SUBCOMMITTEE ON COMMERCE, MANUFACTURING, AND TRADE

LEE TERRY, Nebraska
Chairman

LEONARD LANCE, New Jersey
Vice Chairman
MARSHA BLACKBURN, Tennessee
GREGG HARPER, Mississippi
BRETT GUTHRIE, Kentucky
PETE OLSON, Texas
DAVID B. MCKINLEY, West Virginia
MIKE POMPEO, Kansas
ADAM KINZINGER, Illinois
GUS M. BILIRAKIS, Florida
BILL JOHNSON, Ohio
BILLY LONG, Missouri
JOE BARTON, Texas
FRED UPTON, Michigan *(ex officio)*

JANICE D. SCHAKOWSKY, Illinois
Ranking Member
JOHN P. SARBANES, Maryland
JERRY MCNERNEY, California
PETER WELCH, Vermont
JOHN A. YARMUTH, Kentucky
JOHN D. DINGELL, Michigan
BOBBY L. RUSH, Illinois
JIM MATHESON, Utah
JOHN BARROW, Georgia
DONNA M. CHRISTENSEN, Virgin Islands
HENRY A. WAXMAN, California *(ex officio)*

C O N T E N T S

Page

Hon. Lee Terry, a Representative in Congress from the State of Nebraska, opening statement 1
Prepared statement 3
Hon. Pete Olson, a Representative in Congress from the State of Texas, opening statement 4
Hon. Janice D. Shakowsky, a Representative in Congress from the State of Illinois, opening statement 4
Hon. Jerry McNerney, a Representative in Congress from the State of California, opening statement 5
Hon. Marsha Blackburn, a Representative in Congress from the State of Tennessee, opening statement 5
Prepared statement .....
Hon. Henry A. Waxman, a Representative in Congress from the State of California, prepared statement 83

WITNESSES

Linda Dempsey, Vice President, International Economic Affairs, National Association of Manufacturers 7
Prepared statement 9
Answers to submitted questions 84
Brian Bieron, Executive Director, Public Policy Lab, eBay, Inc. 24
Prepared statement 26
Answers to submitted questions 91
Laura K. Donohue, Professor of Law, Director, Center on National Security and the Law, Georgetown University Law Center 34
Prepared statement 37
Sean S. Heather, Vice President, Center for Global Regulatory Cooperation, Executive Director, International Policy and Antitrust Policy, U.S. Chamber of Commerce 57
Prepared statement 59
Answers to submitted questions 96

SUBMITTED MATERIAL

Letter of September 16, 2014, from Howard Fienberg, Director of Government Affairs, Marketing Research Association, to Mr. Terry and Ms. Schakowsky, submitted by Mr. Terry 77
Letter of April 3, 2014, from Myron A. Brilliant, Executive Vice President and Head of International Affairs, U.S. Chamber of Commerce, to John P. Holden, Assistant to the President for Science and Technology Policy, submitted by Mr. Terry 79

CROSS-BORDER DATA FLOWS: COULD FOREIGN PROTECTIONISM HURT U.S. JOBS?

WEDNESDAY, SEPTEMBER 17, 2014

HOUSE OF REPRESENTATIVES,
SUBCOMMITTEE ON COMMERCE, MANUFACTURING, AND TRADE,
COMMITTEE ON ENERGY AND COMMERCE,
Washington, DC.

The subcommittee met, pursuant to call, at 2:04 p.m., in room 2322, Rayburn House Office Building, Hon. Lee Terry (chairman of the subcommittee) presiding.

Members present: Representatives Terry, Lance, Blackburn, Harper, Guthrie, Olson, Bilirakis, Long, Schakowsky, McNerney, and Barrow.

Staff present: Leighton Brown, Press Assistant; Graham Dufault, Policy Coordinator, Commerce, Manufacturing, and Trade; Melissa Froelich, Counsel, Commerce, Manufacturing, and Trade; Kirby Howard, Legislative Clerk; Paul Nagle, Chief Counsel, Commerce, Manufacturing, and Trade; Michelle Ash, Democratic General Counsel; and Lisa Goldman, Democratic Counsel.

Mr. TERRY. I want to thank all of you for being here. We have a couple of Democrats and a couple of Republicans. I think we are ready to go. So I want to thank our witnesses for being here. I am going to start with my opening statement.

OPENING STATEMENT OF HON. LEE TERRY, A REPRESENTATIVE IN CONGRESS FROM THE STATE OF NEBRASKA

Good afternoon to all. Welcome to our hearing entitled "Cross-Border Data Flows: Could Foreign Protectionism Hurt U.S. Jobs?"

I want to mention, before we get started, that eBay is here to testify today. And I am especially thankful for you that because eBay owns PayPal, which employs about 4,000 people in my district.

We are here today to discuss an emerging trend among many countries around the globe that could potentially have a negative impact on our economy. First of all, what are data flows, and why are they important? The flow of data across borders simply refers to the ability to send an email, a file transfer, video, or other electronic data from one country to another. And because very little business is done today without some form of electronic data, data flows are a big deal for manufacturing, energy, agribusiness, health care, financial institutions, retailers, advertisers, insurance, and tech companies.

But several countries have proposed or enacted restrictions on cross-border data flows or have required companies to locate data

centers within their own borders. For example, Russia has made a law restricting data flows. Brazil proposed a, quote, "civil Internet framework," end quote, that would have authorized the government to require data to be stored in Brazil.

The governments of Indonesia, Singapore, and India have also issued proposals that would either subject cloud computing to additional regulation or require data to remain stored inside respective countries. Sadly, these are but a few of the countries where it is an issue.

Proposals to require local data centers have been aptly named forced localization and come with varying rationales. The European Commission, for example, has argued that localization of data could be a way to promote domestic industry and create jobs. But as we will hear from some of the witnesses today, it is doubtful that such policies would achieve these intended goals. More likely, they would take away the benefits that digital trade brings to that country and to the U.S. companies.

Other proponents of data flow restrictions argue that the revelations concerning U.S. intelligence surveillance justify balkanizing the flow of data.

The United States should send a clear message that forced localization and other restrictions on data flows are commercial regulations that affect businesses, and recent headlines cannot be used to force concessions from U.S. companies that cost us jobs here in the U.S.

Over 300 Federal and State privacy laws are on the books in the U.S., and that proves that we do have privacy policies in the U.S. We have more privacy and risk officers in the U.S. than anywhere else in the world.

Companies are reacting to the market and giving consumers more control, like Facebook's recent policy that permit users to remove themselves from the categories of advertising. And there are very few nations with a better record for the rule of law than the United States. Intelligence surveillance is being tackled, as it should, with input from Congress and our national security agencies.

When it comes to trade, the U.S. cannot allow protectionism. Whether it is under the pretext of privacy or whatever, it threatens U.S. jobs and U.S. competitiveness. Our trade negotiators with USTR and the International Trade Administration have stressed to the counterparts overseas that the negotiations must focus on the commercial flow of data, which is of great value to everyone involved.

There are many pieces that touch on data flows, the Trans-Pacific Partnership, the Trade and Services Agreement, the Transatlantic and Investment Partnership, and the Safe Harbor Framework. We cannot falter in any of these. I am hopeful that Congress will send a unified message to current and future trading partners that trade barriers will not be tolerated, and that we will protect our economic interest in data flows.

I want to thank our witnesses for being here today.

[The prepared statement of Mr. Terry follows:]

PREPARED STATEMENT OF HON. LEE TERRY

Good afternoon, and welcome to our hearing entitled, "Cross-Border Data Flows: Could Foreign Protectionism Hurt U.S. Jobs?"

I want to mention before we get started, that eBay is here to testify today, and I am especially thankful for that because eBay owns PayPal, which has an office of over 4,000 employees in the Omaha area.

We are here today to discuss an emerging trend among many countries around the globe that could potentially have a negative impact on our economy.

First of all, what are data flows and why are they important?

The flow of data across borders simply refers to the ability to send an e-mail, a file transfer, video, or other electronic data from one country to another.

And because very little business is done without some form of electronic data, "data flows" are a big deal for manufacturing, energy, agribusinesses, health care, financial institutions, retailers, advertisers, insurers, and tech companies.

But several countries have proposed or enacted restrictions on cross-border data flows or have required companies to locate data centers within their own borders.

For example, Russia has made a law restricting data flows. Brazil proposed a "Civil Internet Framework" that would have authorized the government to require data to be stored in Brazil.

The governments of Indonesia, Singapore, and India have also issued proposals that would either subject cloud computing to additional regulation or require data to remain stored inside the respective countries. Sadly, these are but a few of the countries where this is an issue.

Proposals to require local data centers have been aptly named "forced localization," and come with varying rationales.

The European Commission, for example, has argued that localization of data could be a way to promote domestic industry and create jobs.

But as we'll hear from some of the witnesses today, it's doubtful that such policies would achieve these intended goals. More likely, they would take away the benefits that digital trade brings to that country and to U.S. companies.

Other proponents of data flow restrictions argue that the revelations concerning U.S. intelligence surveillance justify balkanizing the flow of data.

The United States should send a clear message that forced localization and other restrictions on data flows are commercial regulations that affect businesses, and recent headlines cannot be used to force concessions from U.S. companies that cost us jobs here in the U.S.

Moreover, it is simply not accurate to say that there are not privacy protections in the U.S.

Over 300 Federal and State privacy laws on the books in the U.S. prove otherwise. FTC enforcement proves otherwise. And our marketplace shows otherwise.

We have more privacy and risk officers in the U.S. than anywhere else in the world. Companies are reacting to the market and giving consumers more control—like Facebook's recent policy announcement that permits users to remove themselves from categories of advertising.

And there are few nations with a better record for the rule of law. Intelligence surveillance is being tackled as it should, with input from Congress and our national security agencies.

When it comes to trade, the U.S. cannot allow protectionism-under the pretext of privacy-to threaten U.S. jobs and U.S. competitiveness. Our trade negotiators with USTR and the International Trade Administration have stressed to their counterparts overseas that the negotiations must focus on the commercial flow of data which is of great value to everyone involved.

There are many pieces that touch on data flows: the Trans-Pacific Partnership (TPP), the Trade in Services Agreement (TiSA), the Transatlantic Trade and Investment Partnership (TTIP), and the Safe Harbor Framework. We cannot falter in any of these.

I am hopeful that Congress can send a unified message to current and future trading partners that trade barriers will not be tolerated, and that we will protect our economic interest in data flows.

I thank the witnesses for being here today to shed more light on this issue and for giving our subcommittee the opportunity to spearhead Congress' activity in this area.

Mr. TERRY. I have 1 minute, if anybody wants it.
Gentleman from Texas.

OPENING STATEMENT OF HON. PETE OLSON, A REPRESENTATIVE IN CONGRESS FROM THE STATE OF TEXAS

Mr. OLSON. Thank you, Mr. Chairman, for holding this hearing today.

And thank you to our witnesses for your patience.

As we listen and discuss data policies around the world, it is important to think about the answers to these questions: Number one, in what country has the Internet flourished? In what country, number two, are the majority of Internet headquarters located? Question three, does any other country have anything like Silicon Valley? If not, why not?

I look forward to this discussion today. Thank you. I yield back.

Mr. TERRY. Well done.

I recognize the gentlelady from Illinois.

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

Ms. SCHAKOWSKY. Thank you, Mr. Chairman, and thank you to the witnesses. This is a very complex issue and one that is deserving of this committee's attention.

From a video chat between family members thousands of miles apart, to instant access to news and research, to buying tickets or music or sporting events at the click of a button, the Internet has made our world more interconnected than most would have imagined maybe only 20 years. That growth has helped to support some of the most innovative companies in the world, providing not just entertainment and information, but also supporting millions of jobs here at home.

With the value of e-commerce estimated at $8 trillion per year worldwide and U.S. digital exports in the hundreds of billions of dollars each year, we have to do all we can to promote responsible growth of the Internet.

The U.S. has been the undisputed leader in the development and commercialization of the Internet. But just like at home, people abroad have doubts about the privacy and security practices of American companies. We have seen this most acutely in terms of efforts to restrict cross-border data flows or the transmission of data across national boundaries. Many major economic powers around the world have considered and enacted restrictions on cross-border data flows, and many individuals around the world have sought out alternatives to U.S.-based companies for services from email to e-commerce.

Distrust of American companies and our Government is high. Massive data breaches, like those that occurred at Target and Home Depot, have made data privacy and security a central issue in trade talks with countries and with the European Union. Last year's revelations about the NSA's data collection practices just heightened concerns that already existed in many countries, adding fuel to the fire.

I support the USA Freedom Act, legislation passed in the House in May to limit bulk data collection and require prior judicial approval for collection of sensitive information. The bill would also establish enhanced oversight and transparency mechanisms. The

United States does not have comprehensive privacy or data security protections in place, and I support taking that step.

I am an original cosponsor of H.R. 4400, the Data Accountability and Trust Act, which Mr. Rush introduced earlier this year. That bipartisan bill would require the FTC to establish clear standards for collecting, storing, and disposing of sensitive data and would require entities to inform the public in the event of a breach.

Enactment of the USA Freedom Act and the Data Accountability and Trust Act, as well as steps to strengthen the Electronic Communications Privacy Act, would provide much needed assurances regarding the privacy of data held on U.S. servers. Doing so would, first and foremost, provide peace of mind to Americans concerned about the security of their personal information, and it would also make American businesses even more competitive in the global economy.

I look forward to hearing from our witnesses and getting your perspectives on this important issue and the steps we should take in order to remain the undisputed world leader in the Internet economy.

Do either of the gentlemen wish to—OK. And I would like to yield to Mr. McNerney whatever time is left.

OPENING STATEMENT OF HON. JERRY MCNERNEY, A REPRESENTATIVE IN CONGRESS FROM THE STATE OF CALIFORNIA

Mr. MCNERNEY. I thank the ranking member and also the panel for giving your time and effort on this hearing.

There is a lot of data that flows across our national border, an awful lot of data. That raises questions of privacy, it raises questions of commerce, of national security. Some of our companies that are innovators are saying that our national security posture is hurting their businesses, and that opens up the opportunity for countries across the world to take steps against our country that they say, again, our companies are saying, costing them commerce.

So, as the ranking member said, this is a very complicated issue, and I hope this hearing sheds a little light on that. And then we will be glad to ask questions and try and shed a little bit more light on it.

So with that, I will yield back.

Mr. TERRY. Mr. Barrow, do you have a statement?

Mr. BARROW. No.

Mr. TERRY. You yield back your time?

Ms. SCHAKOWSKY. I yield.

Mr. TERRY. No other statements on—oh, Ms. Blackburn, you are recognized for 5 minutes.

OPENING STATEMENT OF HON. MARSHA BLACKBURN, A REPRESENTATIVE IN CONGRESS FROM THE STATE OF TENNESSEE

Ms. BLACKBURN. Thank you, Mr. Chairman. And I apologize that I am late getting to the committee. We have a few things on the floor and had to do a little bit of work there.

I just am so pleased that we are doing something on the cross-border data flow and the importance that this has in our economy.

I have had the opportunity to work with Peter Welch, and we co-chaired the Privacy Working Group this year. And we brought in a group of business and consumer stakeholders so that we could look a little bit more into this issue and have the time to just do a roundtable discussion. It was important to formulating some opinions and views, and we are appreciative that we had the time to do that.

And we think that it is imperative that our committee seriously examine the restrictions on data flows that are emerging as a primary nontariff trade barrier to the international marketplace that come in the form of digital protectionism and poses a direct threat to U.S. economic development and job creation.

It should be a priority for this Congress and the administration to ensure that U.S. trade agreements cover new and emerging digital technologies. They need to address measures that restrict legitimate cross-border data flow, and they should reexamine emerging policy and legal restrictions that could potentially harm innovation.

I would also like to point out that one of our Privacy Working Group's participants earlier this year was Laura Donohue from Georgetown University Law Center, who is with us today. And it is good to see you again. And we are pleased that you are here to share your thoughts today.

And I yield back my time.

Mr. TERRY. Mr. Guthrie, statement?

Mr. Bilirakis?

Mr. BILIRAKIS. No. Thank you.

Mr. TERRY. All time being yielded back, we will now recognize our witnesses. I am going to introduce you all first. And then, Ms. Dempsey, we will start with you and go from my left to right.

So we are pleased to have Linda Dempsey here today. She is the vice president of international economic affairs for the National Association of Manufacturers.

Mr. Bieron, senior director, eBay Public Policy Lab, thank you.

Ms. Donohue is here. She is a professor of law at Georgetown University Law Center, Center on National Security and the Law. Thank you for being here.

And Mr. Heather, vice president, Center For Global Regulatory Cooperation, executive director, international policy and antitrust policy of the U.S. Chamber.

So now, Ms. Dempsey, you are recognized for your 5 minutes. And there should be the little red light. We keep things easy for us here. Green means go. Yellow means wrap it up. Red means really wrap it up. You are recognized for 5 minutes.

STATEMENTS OF LINDA DEMPSEY, VICE PRESIDENT, INTERNATIONAL ECONOMIC AFFAIRS, NATIONAL ASSOCIATION OF MANUFACTURERS; BRIAN BIERON, EXECUTIVE DIRECTOR, PUBLIC POLICY LAB, EBAY, INC.; LAURA K. DONOHUE, PROFESSOR OF LAW, DIRECTOR, CENTER ON NATIONAL SECURITY AND THE LAW, GEORGETOWN UNIVERSITY LAW CENTER; AND SEAN S. HEATHER, VICE PRESIDENT, CENTER FOR GLOBAL REGULATORY COOPERATION, EXECUTIVE DIRECTOR, INTERNATIONAL POLICY AND ANTITRUST POLICY, U.S. CHAMBER OF COMMERCE

STATEMENT OF LINDA DEMPSEY

Ms. DEMPSEY. Good afternoon, Chairman Terry, Ranking Member Schakowsky, members of the subcommittee. I welcome the opportunity to testify today on behalf of the National Association of Manufacturers. The NAM is the oldest and largest trade association with over 12,000 manufacturing members in every State and every sector of the manufacturing economy. And as this subcommittee knows well, manufacturing is an engine that drives the U.S. economy, directly employing more than 12 million men and women.

A robust and multifaceted trade policy is a key component to growing manufacturing in the United States. With most of the world's consumers outside our borders and over $11 trillion in manufactured goods traded worldwide, exports in sales present enormous opportunity. Where there is a level playing field, manufacturers in the United States are succeeding, as shown by the fact that nearly half of all U.S. manufactured goods are shipped only to our 23 trade agreement partners, with which we also have a manufacturing trade surplus.

To grow more opportunities for manufacturers, we need more trade agreements with more countries, and those trade agreements must be strong, comprehensive, and tailored to meet the challenges of the 21st century.

One of the biggest new commercial challenges globally is the proliferation of new barriers to cross-border data flows and foreign government localization barriers related to information technology infrastructure. The use of digital platforms, including sharing data and information across national borders, is increasingly important to many businesses, particularly manufacturers.

While some of our manufacturers produce and manage those information technology infrastructure, most manufacturers are actually consumers of these technologies. New information technologies and services, such as cloud computing and software as a service, machine-to-machine or M2M technologies, and advanced analytics are advancing manufacturers' ability to grow, be more productive, and more competitive.

These technologies are particularly vital to small and medium-sized businesses, enabling them to acquire information, market their products, and communicate with and serve foreign customers much faster and in a much more cost-competitive manner than ever before.

As information and communication technologies have advanced, however, many countries are moving to restrict the movement of

data and where data can be stored for nothing more than good old protectionist reasons. Manufacturers have seen barriers adopted and considered in many markets, from Brazil, China, India, and Korea, to Indonesia, Nigeria, Vietnam, and Russia. And many governments are claiming national security concerns, although the measures proposed go far beyond the concerns expressed.

For companies that maintain their own servers, the imposition of these types of restraints impede their ability to implement their own business strategies, raises costs, and could potentially force companies to make the choice between doing business in a foreign country or not. These restrictions also undermine cloud computing by reducing economies of scale, forcing service providers to locate servers based on Government mandate, not business decisions. The loss of cost-effective cloud solutions would be particularly harmful to small business manufacturers that increasingly rely on these technologies to market and sell overseas.

Given the importance of this issue, in March the NAM board of directors unanimously approved new policy language urging that disciplines on these practices be included in U.S. trade agreements going forward. We have seen efforts to address these issues globally by APEC and the OECD, bilaterally by the United States and Europe, and with Korea. Yet the trading system has not fully kept place.

The NAM therefore urged the inclusion of negotiating objectives on this issue as part of a new and modernized trade promotion authority. And in January, the NAM welcomed the bipartisan Congressional Trade Priorities Act of 2014, which answered that call by including negotiating objectives to include such disciplines in future agreements.

The NAM is working with U.S. negotiators in support of binding provisions in future trade agreements, including both the final TPP and TTIP talks, that will allow manufacturers and other industries to move, access, and store information across borders, prohibit requirements to establish or use local servers, and ensure nondiscriminatory treatment of digital products and services.

We agree that there can be areas where legitimate exceptions to such binding commitments should be permitted, such as with respect to national security, intellectual property, privacy, and law enforcement. But such exceptions should not be used to create unwarranted or protectionist-based barriers.

We are seeking strong rules in the TPP and TTIP that can set a global model. As manufacturers continue their efforts to rebound after the recession, the last thing they need are additional barriers or unnecessary costs. It is important that the Congress and the administration work together to modernize the trade rules through new trade agreements and a new trade negotiating framework to address these growing barriers.

[The prepared statement of Ms. Dempsey follows:]

NATIONAL ASSOCIATION OF Manufacturers

Leading Innovation, Creating Opportunity, Pursuing Progress.

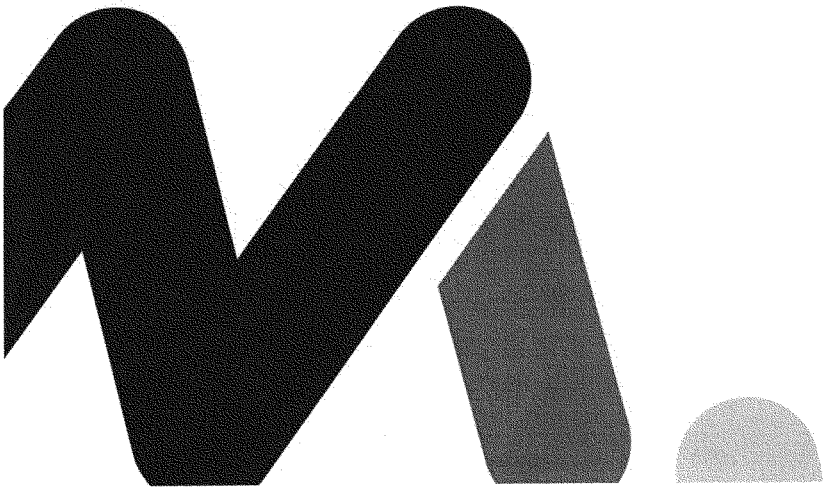
Testimony

of Linda Menghetti Dempsey
Vice President
International Economic Affairs
National Association of Manufacturers
733 10th Street, NW, Suite 700
Washington, DC 20001

House Committee on Energy and Commerce
Subcommittee on Commerce, Manufacturing, and Trade

on "Cross Border Data Flows: Could Foreign Protectionism Hurt U.S. Jobs"

September 17, 2014



Summary of Testimony

- A robust and multi-faceted trade policy that includes new market-opening trade agreements is a key component of growing manufacturing throughout the United States. With 95 percent of the world's consumers outside the U.S. market, exports and sales overseas represent an enormous opportunity for manufacturers in the United States to sustain and grow jobs.
- The use of digital platforms, including sharing data across borders, is increasingly important to the global competitiveness of manufacturers, particularly small manufacturers. The use of such technologies enables manufacturers to lower costs, improve efficiencies and grow exports.
- More than a dozen countries – both developing and developed – have introduced or are actively contemplating new restrictions on the movement of data and information and communications localization rules, from Brazil, China, India and Korea to Indonesia, Nigeria, Vietnam, and Russia. Imposition of such restrictions undermines the global competitiveness of manufacturers in the United States and their ability to sustain and grow manufacturing through reaching new customers outside our borders.
- While recognition of this challenge is growing, the trading system has not fully kept pace. The NAM is seeking a modern Trade Promotion Authority framework that addresses cross-border data flows as a principal negotiating objective and binding commitments in the Trans-Pacific Partnership and Transatlantic Trade and Investment Partnership agreements and through other negotiations.

Testimony

House Committee on Energy and Commerce
Subcommittee on Commerce, Manufacturing, and Trade

***on* "Cross Border Data Flows: Could Foreign Protectionism Hurt U.S. Jobs"**
September 17, 2014

I appreciate the opportunity to testify on behalf of the National Association of Manufacturers – the NAM – which is the nation's largest industrial association with more than 12,000 manufacturing members – small, medium and large. Across the country, manufacturing directly employs more than 12 million women and men and supports over 17 million jobs overall.

Manufacturers contributed $2.08 trillion to the U.S. economy in 2013, the highest level ever. Indeed, manufacturing output has rebounded, after falling from its peak in 2007 of $1.85 trillion to $1.72 trillion in 2009. Since then, manufacturing output has rebounded 18 percent, more than offsetting the decrease during the recession. If U.S. manufacturing were a separate country, it would be the eighth largest economy in the world. Improved energy supplies have played an important role in this growth, as has the substantial investment in new and innovative technologies that manufacturers make. Indeed, manufacturers account for more than two-thirds of private-sector research and development, recognizing that innovation and the development of new technology to manufacture and reach new customers is critical to America's competitiveness in the global economy. Small businesses make up the vast majority of manufacturing firms. Of the 254,941 industrial firms in the United

States in 2011, 79 percent are small businesses with fewer than 500 employees. Nearly 42 percent of these firms have four or fewer employees.[1]

A robust and multi-faceted trade policy is a key component of growing manufacturing throughout the United States. With 95 percent of the world's consumers outside the U.S. market, exports and sales overseas represent an enormous opportunity for manufacturers in the United States to sustain and grow jobs. With world trade in manufactured goods expanding from $4.8 trillion in 2000 to $11.5 trillion in 2012, manufacturers in the United States have been using exports increasingly to fuel growth. In 2013, U.S.-manufactured goods grew to a record high of $1.38 trillion.

More than 97 percent of U.S. companies that export are small and medium-sized businesses with fewer than 500 employees.[2] U.S. employment in trade-related jobs grew six and a half times faster than total employment between 2004 and 2011.[3] Jobs linked to exports pay, on average, is 18 percent more than other jobs.[4]

---

[1] The Manufacturing Institute, "Small Businesses Dominate the Industrial Landscape" (April 2014), accessed at http://www.themanufacturinginstitute.org/Research/Facts-About-Manufacturing/Economy-and-Jobs/Company-Size/Company-Size.aspx.

[2] U.S. Department of Commerce, **U.S. Exporters in 2011: A Statistical Overview**, accessed at http://www.trade.gov/mas/ian/smeoutlook/tg_ian_001925.asp.

[3] Baughman and Francois, **Trade and American Jobs, The Impact of Trade on U.S. and State Level Employment: An Update** (2010), accessed at http://businessroundtable.org/uploads/studies-reports/downloads/Trade_and_American_Jobs.pdf; Business Roundtable, **How the U.S. Economy Benefits from International Trade and Investment**, accessed at http://businessroundtable.org/sites/default/files/legacy/uploads/general/BRT_State_Studies_-_US_Total.pdf.

[4] Riker, **Do Jobs in Exports Still Pay More? And Why?**, U.S. Department of Commerce Manufacturing and Services Brief (July 2010), accessed at http://trade.gov/mas/ian/build/groups/public/@tg_ian/documents/webcontent/tg_ian_003208.pdf.; see also

Whether manufacturers sell to customers down the street, across the country or around the world, manufacturers big and small compete in a highly competitive global economy. Many manufacturers in the United States participate in global supply chains that connect large and small companies and consumers across the world.

To grow America's manufacturing, the NAM is advocating a trade policy that:

- Opens markets overseas;
- Ensures our manufacturers are cost-competitive globally; and,
- Makes sure all our trading partners – and the United States – play by the rules of the global trading system.

Where there's a level playing field in overseas markets, manufacturers in the United States are succeeding. America's existing network of 20 free trade agreement partners account for less than ten percent of the global economy but purchase nearly half of all U.S. manufacturing exports – supporting millions of jobs across the country. In fact, the United States enjoys a nearly $60 billion manufacturing trade surplus with its trade agreement partners, compared with a $508 billion trade deficit with the rest of the world.[5]

To grow more opportunities for our nation's manufacturers, we need more trade agreements with more countries. And those trade agreements must be tailored to meet the challenges of a 21st century economy. The NAM is therefore a strong supporter of comprehensive, market-opening and high standard

[5] *See*, NAM Trade Toolkit: U.S. Manufacturing and Trade Data, accessed at www.nam.org/issues/Toolkits/Trade-Toolkit/Learn-More/Data.aspx.

outcomes in the major ongoing U.S. trade negotiations in the Asia Pacific and Europe – the Trans-Pacific Partnership (TPP) and the Transatlantic Trade and Investment Partnership (T-TIP).

While manufactured goods exports have more than doubled since Congress last approved trade negotiating authority in 2002, manufacturers face real and growing barriers overseas, most prominently in countries with which we have not negotiated free trade agreements.

One of the biggest new commercial challenges globally is the issue before the Subcommittee today – the growth of new barriers to the movement of data and information across national borders and foreign government localization barriers that seek to require the use of local information technology infrastructure. These restrictions undermine the global competitiveness of manufacturers in the United States and their ability to sustain and grow manufacturing through reaching new customers outside our borders.

The Importance of Cross-Border Data Flows and ICT Infrastructure Issues to Manufacturers in the United States

The use of digital platforms, including sharing data and information across borders, is increasingly important to industries across many different economic sectors, particularly a broad range of manufacturing industries.[6] While some manufacturers produce and manage the information and communications technology (ICT) infrastructure, most manufacturers, like other businesses, are major consumers of these new technologies and equipment, which have been an

[6] Matthieu Pélissié du Rausas, James Manyika, Eric Hazan, Jacques Bughin, Michael Chui, Rémi Said, Internet matters: The Net's sweeping impact on growth, jobs, and prosperity, McKinsey Global Institute, May 2011.

important driver of productivity, competitiveness and new economic opportunity across the globe. New ICT products and services, such as cloud and "machine to machine" technologies, are advancing manufacturers' ability to grow and reach new markets more efficiently. The importance of ICT products and services is particularly vital to many small and medium-sized businesses. ICT technologies enable small business to acquire information, market their products and communicate and serve foreign customers much faster and in a more cost-effective manner than ever before. As a result, small businesses are better able to expand sales overseas, creating new demand that is served by growing manufacturing and jobs domestically.[7]

Let me provide a few examples of why the issues of digital trade and data flows are so important to a broad range of manufacturers:

- Manufacturers throughout America increasingly use digital platforms that depend on the unencumbered flow of data across borders to reach new customers, run manufacturing and internal operations, and manage global supply chains.
- Manufacturers are among the many businesses benefitting from the "software as a service" (SAAS) revolution. SAAS allows firms large and

[7] As documented in **Ahead of the Curve: Lessons on Technology and Growth From Small Business Leaders**,[7] by the Boston Consulting Group, information and communications technology has a powerful impact on the growth and success of small and medium sized enterprises (SMEs) from the United States and Germany to China, India and Brazil. The report found that SMEs that were technology leaders created twice as many jobs and increased revenue 15 percent in the past three years than those SMEs that lagged behind in the adoption of new technologies. This report shows that SMEs across these five economies could create $770 billion in new revenue and add about 6.2 million new jobs with the increased adoption of new technologies. **Ahead of the Curve**, Boston Consulting Group (Oct. 5, 2013), accessed at https://www.bcgperspectives.com/content/articles/technology_software_globalization_ahead_curve_lessons_technology_growth_small_business_leaders/.

small to improve operational efficiency and cut infrastructure costs by shifting computation, software, data access and storage resources securely to cloud-based service providers. Common cloud-based services used by manufacturers range from email and file storage to sophisticated sales, e-commerce and human resources applications.

- Manufacturers are also turning to advanced analytics to extract insights from the vast quantities of data generated by our global fleet of manufactured equipment– including jet engines, gas turbines, locomotives and other industrial technologies. These insights – made possible through cloud computing and cross-border data flows – will serve as a further catalyst for growth and innovation as they improve productivity, efficiency and reliability.
- Manufacturers are also at the forefront of building "machine to machine" technologies (M2M or the Internet of Things) to transfer data remotely between machines that can do everything from locating lost devices and machines through GPS-driven navigation and tracking to providing key information regarding product usage, yield, performance and maintenance.

The use of such technologies has enabled manufacturers to compete more successfully in a tough global economy by lowering costs, improving efficiencies and growing exports. To be able to grow America's share of the $11 trillion global market in traded manufactured goods, manufacturers must be confident in their

ability to use digital platforms and to move data and information securely across borders and to be able to store data as their business requires.

Challenges to the Free-Flow of Data and the Use of ICT Technologies

As ICT technologies have advanced, however, many countries are moving to restrict the movement of data and where data can be stored – for reasons that have a lot to do with good old-fashioned protectionism. Around the world, more than a dozen countries – both developing and developed – have introduced or are actively contemplating introducing data localization laws. Over the past several years, manufacturers have seen new barriers proposed or considered in many markets, from Brazil, China, India and Korea to Indonesia, Nigeria, Vietnam and Russia. In some cases, governments are claiming national security concerns, although the measures they are proposing and implementing go far beyond the concerns expressed.

For example, Brazil had proposed a "Civil Internet Framework" that, among other things, would have authorized Brazil's Executive Branch to require data relating to the Brazilian operations of both domestic and international companies, as well as Brazilian citizens, to be stored in Brazil. While this forced data localization language has since been stripped from the Framework, there continue to be reports that such legislation may be reintroduced.

Similarly with South Korea, the U.S. government and U.S. industry have raised concerns with legislation proposed by South Korea's Ministry of Science, Information and Communications Technology and Future Planning (MSIP) to the National Assembly that would provide a jurisdictional basis for the regulation of

cloud computing and could potentially impose additional regulations on global technology. While MSIP modified its original proposal to address many of the issues raised by the United States, concerns remain and manufacturers continue closely monitoring the progress of this proposal in the National Assembly. Notably, the Korea-U.S. Free Trade Agreement (KORUS FTA) contains language recognizing that the Parties should not impose unnecessary barriers to data flows.[8]

In 2012, Indonesia issued Regulation 82, "Operation of Electronic Systems and Transactions," to the 2008 Law 11 on Electronic Information and Transactions. The regulation requires extensive certification requirements and restrictions on electronic systems providers that provide services for the "public use," which has not been fully defined. Such restrictions include maintaining Indonesian data centers and requiring any data relating to electronic transactions be stored in Indonesia.

In February 2014, the Indian National Security Council proposed significant new restrictions on cross-border data flows, including requiring that all communications between users in India stay in India and be stored locally on Indian servers.[9]

Industry has also raised serious concerns over a draft decree issued by Vietnam's Ministry of Information and Communication that would impose

[8] "Recognizing the importance of the free flow of information in facilitating trade, and acknowledging the importance of protecting personal information, the Parties shall endeavor to refrain from imposing or maintaining unnecessary barriers to electronic information flows across borders." KORUS FTA, Art. 15.8.

[9] Thomas K. Thomas, "National Security Council proposes 3-pronged plan to protect Internet users," The Hindu, Feb. 13, 2014, accessed at www.thehindubusinessline.com/features/smartbuy/national-security-council-proposes-3pronged-plan-to-protect-internet-users/article5685794.ece.

registration and licensing requirements on providers of information technology services. The decree would also restrict cross-border cloud computing and data services.

These and similar types of barriers undermine U.S. commercial opportunities overseas, impede the ability of manufacturers to conduct business and weaken our competitiveness. For companies that maintain their own servers, the imposition of cross-border data restraints or server localization requirements impedes their ability to implement their own business strategies, raises costs and would potentially force companies to make the choice between doing business in a particular country and housing their data on local servers or choose not to do business because they do not want the risk of data being held locally.

In addition, restrictions on cross-border data flows, including local storage requirements, undermine cloud computing by reducing economies of scale, forcing service providers to locate servers based on government mandate, rather than business decisions. Local storage requirements may require the deployment of duplicative technology resources in countries where providers would not otherwise plan to deploy those resources. As well, cross-border data flow restrictions and server localization requirements undermine the ability of cloud-based providers to achieve critical economies of scale and maximize server capacity. Typically, cloud providers offer services to many companies at the same time and may store data securely across borders in order to take advantage of economies of scale. The economic and secure benefit of innovative cross-border services that are in high demand, such as cloud technologies, is

diluted when countries impose policies which fragment these services into nation-based solutions lacking the economic benefits of scale, high resource utilization rates and demand aggregation, and the legal certainty and consistency necessary to provide a truly global service that benefits all types of customers. The loss of a cost-effective and easily manageable cloud technology solution would be particularly harmful to small businesses that are increasingly relying on cloud solutions to market and sell overseas.

Modernizing ICT Trade Rules

Given the growing importance of this issue to manufacturers in the United States, in March 2014, the NAM Board of Directors unanimously approved new policy language seeking that new trade agreements include "commitments to liberalize cross-border data flows of information and access to digital products and services, and prohibit related localization requirements, such as requirements to use local data information infrastructure and storage."

Efforts to address these issues have also been undertaken globally. In 2008, the Asia Pacific Economic Cooperation (APEC) forum issued a "Digital Prosperity Checklist" that recognized the importance of the "free flow of information."[10] APEC followed that initiative with both the APEC Innovation Principles in 2011 and the APEC Privacy Framework in 2012 that explicitly emphasized the importance of these issues.[11]

---

[10] Digital Prosperity Checklist, APEC (Nov. 2008), accessed at http://mddb.apec.org/documents/2010/TEL/TEL41-DSG-WKSP1/10_tel41_dsg_wksp1_003.pdf.
[11] See APEC, Promoting Effective, Non-Discriminatory, and Market-Driven Innovation Policy (Nov. 2011), accessed at http://www.apec.org/Meeting-Papers/Leaders-Declarations/2011/2011_aelm/2011_aelm_annexA.aspx; APEC Privacy Framework Pathfinder,

The Organisation for Economic Cooperation and Development (OECD) developed "Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data" in July 2013 that established a framework that supports cross-border data flows.[12]

As well, in April 2011,[13] the United States and European Union (EU) agreed to a set of trade principles on ICT services that highlight the importance of ensuring the free flow of data across borders and avoiding localization requirements.[14] As noted previously, the KORUS FTA included general provisions on this issue, as well as more specific language relating to financial services.

While recognition of this issue has been growing, the trading system has not fully kept pace. As the NAM and nine other associations explained in a letter to United States Trade Representative Ambassador Froman, "current trade rules are insufficient to ensure that borders remain open to data flows and services

---

accessed at http://mddb.apec.org/documents/2010/TEL/TEL41-DSG-WKSP1/10_tel41_dsg_wksp1_003.pdf

[12] OECD Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data (July 11, 2013, accessed at http://www.oecd.org/sti/ieconomy/privacy.htm.

[13] United States-European Union Trade Principles for Information and Communication Technology Services (April 4, 2011) (U.S.-EU ICT Trade Principles), accessed at http://www.ustr.gov/about-us/press-office/press-releases/2011/april/united-states-european-union-trade-principles-inform;

[14] In particular, the U.S.-EU ICT Trade Principles state:

> 3. Cross-Border Information Flows: Governments should not prevent service suppliers of other countries, or customers of those suppliers, from electronically transferring information internally or across borders, accessing publicly available information, or accessing their own information stored in other countries.
> 4. Local Infrastructure: Governments should not require ICT service suppliers to use local infrastructure, or establish a local presence, as a condition of supplying services. In addition, governments should not give priority or preferential treatment to national suppliers of ICT services in the use of local infrastructure, national spectrum, or orbital resources.

U.S.-EU ICT Trade Principles (April 4, 2011).

receive non-discriminatory treatment in key markets."[15] The NAM, along with others in the business community, is working to help countries build a new architecture to address these issues.

In particular, the NAM urged the inclusion of this issue as part of a new and modernized authorization of Trade Promotion Authority[16] and welcomed the Bipartisan Congressional Trade Priorities Act of 2014, which urges negotiators "to ensure that governments refrain from implementing trade related measures that impede digital trade in goods and services, restrict cross-border data flows, or require local storage or processing of data."[17]

The NAM is also pressing for binding provisions in future trade agreements, including both the final TPP and T-TIP agreements that are currently in negotiation. In particular, the NAM is seeking binding commitments in these negotiations that will allow manufacturers and other industries to transfer, access, process or store information across borders; prohibit the imposition of restrictions that would require the establishment or use of local servers generally or as a condition of access to the market; and ensure non-discriminatory treatment of digital products and services.

We agree that there can be areas where exceptions to such binding commitments should be permitted, such as with respect to legitimate national security, intellectual property, privacy and law enforcement. Such exceptions should not, however, be used to create unwarranted or protectionist-based

[15] Letter to Ambassador Michael Froman (Sept. 26, 2013).
[16] NAM Trade Promotion Priorities (2013), accessed at http://www.nam.org/Issues/Trade/Trade-Promotion-Authority.aspx.
[17] H.R. 3830, the Bipartisan Congressional Trade Priorities Act of 2014, accessed at http://waysandmeans.house.gov/tpa/.

barriers to cross-border data flows or the use of ICT infrastructure. Thus, any exceptions should not be unnecessarily restrictive or constitute a disguised restriction on trade; and, should be consistent with and no broader than the general exceptions (Article XIV) of the General Agreement on Trade in Services.

Both the TPP and T-TIP agreements represent an important opportunity to modernize the international rules on ICT issues in ways that can advance manufacturers' global competitiveness and ensure that markets are open. Even more broadly, the outcomes in these agreements, if successful, can be a model for a new global architecture. Adoption of such disciplines can help countries increase their attractiveness to foreign investment that relies increasingly on access to ICT technologies, services and networks.

Conclusion

All manufacturers with cross-border investment and sales need to see policies put into place that ensure that their data can move across borders, that electronic commerce is accepted and that prohibit requirements to localize technology (such as servers) in any one country. It important that the U.S. government lead efforts globally, including as part of the TPP and T-TIP, to modernize the trade rules that relate to ICT technology and services to ensure the ability of manufacturers in the United States to grow through greater access to trade and consumers overseas.

-NAM-

Mr. TERRY. Thank you.
Mr. Bieron, you are recognized for 5 minutes.

STATEMENT OF BRIAN BIERON

Mr. BIERON. Chairman Terry, Ranking Member Schakowsky, and members of the subcommittee, thank you for giving eBay Inc. the opportunity to testify on the role of cross-border data flows in promoting commerce, economic growth, and opportunity.

Our company is a truly global business. 60 percent of our marketplace business is outside the United States. We serve over 152 million PayPal users in 2003 countries.

EBay Inc. is using technology to power global trade. The eBay marketplace, PayPal payment service, and eBay Enterprise enable hundreds of thousands of U.S. entrepreneurs and small businesses, as well as midsized and large business, to reach customers around the world. This is transforming trade by allowing Main Street businesses to directly take part in globalization, reaping the benefits of markets previously only open to the largest global companies.

The 21st century global economy is built on data flows. Every business that operates internationally depends on access to digital services, including technology, logistics, finance, and professional services. The Internet alone powers 21 percent of GDP growth in advanced economies and facilitates $8 trillion in e-commerce. It drives global economic and social progress, and the U.S. Internet industry leads the way. But it should be clearly understood that much of the benefit is gained by traditional industries and businesses, 75 percent according to McKinsey.

So, not surprisingly, America's leading industries are united in their concerns about data protectionism. But our unique experience at eBay and PayPal leads us to stress how the Internet and mobile technology are now powering global trade by small and micro-businesses. These entrepreneurial traders, such as Tracey Johnson, who employs three people in Valley, Nebraska, or Esther Ben Porat, who employs 12 people in Lincolnwood, Illinois, they will be undermined in their businesses if open cross-border data flows are restricted.

My team conducts research on the growth of global trade by technology-enabled small businesses. In brief, the Internet and platforms like eBay and PayPal are revolutionizing this global trade. In the U.S., only 4 percent of traditional small businesses export. On eBay, 95 percent export. Traditional small business exporters reach an average of 2 markets a year. On eBay, the average small business exporter reaches 30 markets a year.

Technology-enabled small businesses survive at a higher rate, and newcomers capture a larger share of the overall market than in the traditional offline world. The global trade regime is literally changing before our eyes, as enterprises that historically were too small to break into global trade can now directly participate.

This new inclusive globalization depends on four components that make up what we call the Global Empowerment Network. They are, one, access to the Internet; two, access to the global services that exist on top of the Internet; three, an efficient small package shipment logistics network; and, four, an educational system for small businesses to learn about online opportunities. Each of

these components is undermined by data restrictions requiring businesses to locate data centers, store data, or process data in a specific country. These restrictions impose meaningful economic and security harms.

These are nontariff trade barriers. Like all trade barriers, they lead to inefficiencies, higher prices, and harms to businesses and consumers. They harm U.S. businesses. But just as importantly, they hurt businesses and consumers in the markets that employ them.

Data localization proposals in countries like Brazil, China, the EU, India, Indonesia, Korea, Vietnam have been estimated to impact GDP from potentially a 10th of a percent to 1.7 percent, depending on the market. Small and midsized technology-enabled business in each of those countries are threatened.

Of course, the U.S. impact is key as well. The U.S.-based global corporations will be harmed by the entire range of data protectionist proposals. Costs are imposed, inefficiencies are forced into the system, and opportunities are lost. But now, because of Internet-enabled global commerce, small and midsized businesses in every State and region of the United States will be impacted.

Today we are witnessing the dawn of a new era of globalization. Small and midsized businesses contribute to their local economy and regularly serve customers around the world at the same time. This is good economics because it means more growth and wealth, and it is good for society because it means a more inclusive form of globalization.

U.S. leadership is key to maintaining open global data flows and pushing back on data protectionism. This should be a top trade policy priority, to protect and promote growth at all levels. And I look forward to answering any questions.

[The prepared statement of Mr. Bieron follows:]

TESTIMONY OF

Brian Bieron

Executive Director, Global Public Policy Lab

eBay Inc.

BEFORE THE

United States House of Representatives

Committee on Energy and Commerce

Subcommittee on Commerce, Manufacturing, and Trade

Cross Border Data Flows: Could Foreign Protectionism Hurt U.S. Jobs

PRESENTED

Rayburn House Office Building, Room 2322

September 17, 2014

1:30 PM

Chairman Terry, Ranking Member Schakowsky, and members of the Subcommittee, I would like to thank you all for giving eBay Inc. the opportunity to testify today on the very important topic of the role of cross border data flows in promoting global commerce, economic growth and opportunity. Our company is a truly global business. 60% of our Marketplaces business is international. Our platforms enable hundreds of thousands of U.S. entrepreneurs, small businesses, as well as mid-size and large businesses, to reach customers around the world. We empower over 148 million buyers globally on our marketplaces, as well as 152 million PayPal account holders, with users in 203 countries. This is a new kind of a global trade that is truly beneficial for Main Street businesses across America, and underpinning this new kind trade is uninhibited cross border data flows and the Internet.

eBay Inc. serves as a platform for the growth and development of technology-enabled small business exporters. Founded in 1995, eBay Inc. connects millions of buyers and sellers globally on a daily basis through eBay, one of the world's largest online marketplaces; PayPal, which enables individuals and businesses to securely, easily, and quickly send and receive online payments around the world; and eBay Enterprise, which enables omni-channel commerce, multichannel retailing and digital marketing for global enterprises. eBay Inc. is in the business of empowering businesses of all sizes to engage in the global marketplace through technology tools and platforms to directly engage with customers wherever they are.

eBay Inc. is an Internet and mobile technology-based business, but in the 21st Century global economy, every business that operates internationally in any significant scale depends on access to, and transmission of, digital goods and services, including logistics, online services, distribution networks, finance and professional services. The Internet accounts for 21% of GDP growth in advanced economies and facilitates $8 trillion each year in e-commerce. Led by our global leaders in the Internet industry,

the U.S. captures more than 30% of global Internet revenues and more than 40% of net income. But data moving across borders is not just an Internet industry phenomena, it impacts every business, including manufacturers, agricultural businesses, and financial services providers. McKinsey reports that 75% of the impact of the Internet is being realized by traditional industry.[i] The US International Trade Commission, in its recently released report on digital trade, estimates that digital trade has already boosted U.S. gross domestic product by 3.4 to 4.8%, through enhanced productivity and reduced international trade costs, and the effect on U.S. total employment ranged from no change to an increase of 2.4 million full-time equivalents.[ii]

The issue of cross border data flows impacts an even wider swath of American businesses, because it is not just important to big, global businesses that have operations in multiple countries; the household names of the trade debates that everyone knows. Cross border data and the Internet lie at the heart of a new trade phenomenon driven by small and micro-businesses that are engaging in trade. And, these small businesses are at risk of harm if open cross-border data flows are restricted or shut down.

My team at eBay Inc. has spent the last four years conducting research on the growth of global trade by technology-enabled small businesses.[iii] The findings from our research are quite extraordinary. In the US, only about 4% of traditional businesses export. However, our research demonstrates that over 95% of the US-based small businesses using our eBay Marketplaces platform engage in exporting.[iv] In addition, traditional US businesses that export reach on average 2-3 different markets per year, while US-based small and mid-size business exporters using eBay reach over 30 markets per year.

Our data points to technology-enabled businesses being healthier than their offline counterparts. Only 45% of traditional US businesses survive their first four years; nearly 65% of the new US-based

businesses that use our platform, survive their first four years. In short, technology-enabled businesses export at a higher rate to more countries and with a higher survival rate than their offline counterparts. Finally, technology-enabled trade is not only more robust than traditional trade, it is also more inclusive. The largest 5% of businesses in the US account for over 90% of the total exports. The largest 5% of US technology-enabled businesses on the eBay Marketplace account for less than 20% of the total export market share. Businesses of all sizes are competing and winning online; their growth is coming from overseas buyers.

Alongside these impressive statistics there are many excellent examples of small business success stories including:

- Tracey Johnson from Valley, Nebraska, sells jewelry and hair care products to consumers all over the world through eBay and PayPal. Tracey sells to dozens of countries worldwide, including small countries like Malta. He said that his ability to export across the globe has increased his sales.

- Esther Ben Porat lives and works in Lincolnwood, Illinois. Her business focuses on commercialized fabrics. She sells her products around the world using the eBay platform and her own website. Esther's business has grown around 10-15% annually. She has been able to hire 6 employees and has annual revenues of about $3 million.

- Finally, Jamie Wankum lives in North Sioux City, South Dakota and before starting his business he managed international sales for Gateway Computers. Jamie left Gateway after 15 years to

start his own business focused on the electronics sector. He has grown his business from a local shop to a global enterprise with around $3 million in annual revenue.

The kind of cross-border trade being done by these, and hundreds of thousands of other "micro-multinationals" spread across America, is growing rapidly. A research report from Progressive Economy finds that low-value or "micro" US exports increased by 103% between 2005 and 2010, more than twice the increase for all exports.[v] Moreover, the 2013 World Economic Forum (WEF) Enabling Trade report found that the use of technology platforms can reduce the burdens small businesses face when selling overseas, increasing cross-border small business sales by 60-80%.[vi]

This new more inclusive version of globalization depends upon four key components that make up what we refer to as the Global Empowerment Network: 1) the Internet; 2) the services that exist on top of the Internet; 3) the small shipments logistics network that carries the physical products being traded by technology-enabled small businesses; and 4) the educational infrastructure for small businesses to learn about online opportunities and be educated on how to leverage online tools. Restrictions on cross border data flows threaten to diminish the benefits of all of these factors.

Some governments around the world have responded to concerns about trust in the Internet ecosystem, usually in the form of perceived privacy or security threats, by proposing laws that would require Internet companies to locate storage infrastructure (generally in the form of data centers) in-country. Some governments have even gone so far as to require organizations to process all data locally. These restrictions would greatly limit the many benefits of the Internet that have been laid out above. Imposing data localization requirements on Internet-enabled businesses is problematic from both an economic and security perspective.

Localization requirements undermine the economic benefits of the Internet, particularly for small enterprises and consumers. Small enterprises are generally less able to afford the additional costs that data localization imposes and would be less able to engage in global trade using the Internet. Large businesses will be forced to make decisions based on regulations rather than price, resulting in inefficiencies that give rise to higher prices which are passed on to local small businesses and local end consumers. In this particularly sensitive time in which regional economies are still reeling from the recession, these types of non-tariff barriers to trade only serve to further slow economic recovery.

Professor Anupam Chander at UC-Davis Law School estimates that building a data center in Brazil costs $60.9 million on average, while building one in Chile and the United States costs $51.2 million and $43 million, respectively. Moreover, Professor Chander describes estimates the costs of data center operation at $950,000 in Brazil, $710,000 in Chile, and $510,000 in the United States each month.[vii] The European Centre for International Policy Economy, an independent think tank, estimates that data localization legislation in Brazil, China, the EU, India, Indonesia, Korea, and Vietnam could impact GDP from anywhere between -.1% to -1.7% depending on the market.[viii] So really, restrictions on cross border data flows only serve to harm the local economy.

Moreover, security is actually diminished as a result of data localization policies. Data management and security is paramount to Internet businesses, and the selection of where to build data centers is heavily focused on security. Security networks are only as vulnerable as their weakest link. Proliferating data centers will reduce the ability of businesses to maintain

security, putting the integrity of the systems in jeopardy, and creating targets for security threats. Robust security and privacy systems have been put in place by major Internet companies. eBay Inc. for example processes over 70,000 requests from law enforcement each year, and has a strict policy of responding to these requests within 20 days. If governments are concerned about resolving security concerns associated with the Internet they should continue to work with intermediaries like eBay and should improve the Mutual Legal Assistance Treaty (MLAT) process, which provides a system of review for law enforcement requests and prevents abuse.

Localization requirements will not achieve the shared goal of increasing security and trust in the Internet. The Internet's architecture is built upon a multi-stakeholder governance model, and that same model can be used to setup a positive framework for privacy and security on the Internet. Governments, industry, users, and technical experts can work together to reconcile regulatory concerns with the practicalities of data management. eBay Inc. is fully committed to working with governments around the world to ensure trust in the Internet ecosystem.
Another point worth noting is that localization barriers are actually proliferating most among some of the larger and more developed countries. G20 countries are responsible for 65 percent of the protectionist measures, and at the same time, they are also the countries which are the worst affected by protectionism.

Finally, it is key to realize that our discussion today about cross border data flows is not merely about business or policy; it is about people. Globalization and trade are fundamental realities of the world we live in. Unfortunately, a significant number of people have not yet been able to directly take part in the global marketplace because they own or work in businesses that are too small. Global trade has been

the purview of the giant multinational companies that could achieve global scale. But now the Internet, and the global data-based businesses and platforms that underpin 21st Century commerce, are enabling small business and consumers, for the first time, to truly enjoy the benefits of the global market. We sit at the dawn of a new era of globalization that is far more inclusive than the one that preceded it. A future where millions of small businesses from across the US can contribute to their local economy, but also increase revenue through access to customers around the world. This is good economics because it means more growth and wealth, and it is good for society because it means a more inclusive future. We need to make the right policy choices to achieve this future.

Mr. Chairman, ranking member Schakowsky, members of the subcommittee, we respectfully submit this testimony and pledge to work with you to ensure that US small businesses and consumers can see the true benefits from the Internet.

---

[i] McKinsey Global Institute, Internet Matters: The Net's Sweeping Impact on Growth, Jobs, and Prosperity (May 2011) available at: http://www.mckinsey.com/insights/high_tech_telecoms_internet/internet_matters

[ii] U.S. International Trade Commission, Digital Trade in the U.S. and Global Economies, Part 2 available at: http://www.usitc.gov/publications/332/pub4485.pdf

[iii] The Full range of research can be found here: http://www.ebaymainstreet.com/commerce-3

[iv] Enabling Traders to Enter and Grow on the Global Stage available here: http://www.ebaymainstreet.com/sites/default/files/EBAY_US-Marketplace_FINAL.pdf

[v] Gresser, Edward. "Lines of Light: Data Flows as a Trade Policy Concept." (2012).

[vi] World Economic Forum, Enabling Trade (2013)

[vii] Anupam Chander, Breaking the Web: Data Localization vs. the Global Internet forthcoming Emory Law Journal (April 2014) available at: http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2407858

[viii] Matthias Bauer, Hosuk Lee-Makiyama, Erik van der Marel, Bert Vershelde, The Costs of Data Localization: Friendly Fire on Economic Recovery (March 2014) available at: http://www.ecipe.org/media/publication_pdfs/OCC32014__1.pdf

Mr. TERRY. Thank you, Mr. Bieron.

Professor Donohue, you are now recognized for your 5 minutes.

STATEMENT OF LAURA K. DONOHUE

Ms. DONOHUE. Thank you very much. I would like to thank you. Thank you, Ranking Member Schakowsky, and also members of the committee for inviting me here today.

As you have noted, U.S. Companies dominate the digital space: Web browsing, search, email, social networking, traditional computing devices, smartphones, tablets. There are few foreign analogs to Google, Facebook, LinkedIn, Twitter, Instagram, Pinterest, myriad others who could compute with us on a global basis. But the U.S.' position is now imperiled.

Documents released over the past year detailing the National Security Agency's call record program and the interception of content under the Foreign Intelligence Surveillance Act directly implicated U.S. high technology companies in Government surveillance. The result has been an immediate and detrimental impact on U.S. industry.

The first documents revealed that the Government had served orders on Verizon, directing the company to turn over telephony metadata under Section 215 of the USA Patriot Act. The following day, The Guardian published classified slides on PRISM, detailing how the NSA had intercepted email, video, and voice chat, videos, photos, stored data, Voice over Internet Protocol, file transfers, video conferencing, online social networking details. And the companies read like a who's who of U.S. Internet giants: Microsoft, Yahoo, Google, Facebook, PalTalk, YouTube, Skype, AOL, and Apple.

Slides showing the extent of so-called upstream collection similarly stunned the public, showing that the NSA had bypassed companies' encryption, intercepting data as it transferred between servers and the cloud, and it had obtained millions of email address books.

Beyond these revelations, reports show that the NSA has at times posed as U.S. companies without their knowledge in order to gain access to foreign targets. I have documented all of this information in my written remarks. Three points follow. First, these programs have cost the United States billions of dollars. Second, they have pushed foreign countries to erect trade barriers through data localization laws. And, third, they have undermined U.S. national security.

This subcommittee is uniquely poised to address the problem by supporting changes to FISA and U.S. privacy laws. It can also push for the insertion of economic and commercial representation throughout the national security infrastructure to prevent this situation from occurring again.

So, first, the economic impact. In short, billions of dollars are on the line because of worldwide concern that the services provided by U.S. information technology companies are neither secure nor private. Perhaps nowhere is this more apparent than in cloud computing, arguably one of the most important industrial sectors for the future. The Information Technology and Innovation Foundation estimates that declining revenues for U.S. cloud computing could

reach more than $35 billion over the next 3 years. Other commentators have put the losses as high as $180 billion by 2016, unless something is done to restore confidence in U.S. industry.

The impact extends to high technology. Cisco, Qualcomm, IBM, Microsoft, and Hewlett-Packard have all claimed declining revenues as a result of the NSA programs. Servint, a Web-hosting company next door here in Virginia, reports that its international clients have dropped by 50 percent.

As a senior analyst at the Information Technology and Innovation Fund explained, it is clear to every single tech company that this is affecting their bottom line. In return, companies have had to spend billions of dollars on new encryption. And even as U.S. companies are losing money, foreign companies are seeing their revenues increase.

The NSA's involvement in these programs also revealed the extent to which it had became embedded in the architecture of the Internet itself. And as a result there has been a backlash that has led some commentators to raise concern that the Internet will never be the same. At risk is the balkanization of the Internet, undermining a traditional culture of open access and increasing the cost of doing business.

As of today, China, Greece, Malaysia, Russia, South Korea, Venezuela, Vietnam, and others have already implemented data localization requirement laws. Turkey has introduced new privacy regulations, preventing the transfer of personal data overseas. Other countries, such as Argentina, Brazil, India, and Indonesia, are actively considering new data localization laws. Germany and France are considering a Schengen routing system, retaining as much online data in the European Union as possible.

The Snowden release has further implicated our multilateral and bilateral trade negotiations. Two of the most important underway are TTIP, the Transatlantic Trade and Investment Partnership, and the Trans-Pacific Partnership.

Although the U.S. Trade Representative is trying to put data protections on the table for the TTIP negotiations, the EU has steadfastly resisted this. And as long as the European public is strongly opposed to giving the United States access to European data the future does not bode well for our efforts.

TPP, in turn, accounts for about 40 percent of global GDP, about ⅓ of world trade. Two of our objectives in those negotiations are directly implicated by the Snowden releases: e-commerce, telecommunications, and intellectual property rights. The NSA programs weaken the USTR's hand with regard to open access and safeguards against cyber surveillance.

This subcommittee has an opportunity to make a difference. The most important thing you could do is to curb the NSA's authorities under the Foreign Intelligence Surveillance Act. In January 2014 the President announced the telephony metadata program would be discontinued within 2 months. As of last month, it was continued for another 90 days. The Section 702 program is more complicated. Overseas collection from non-USP's is a concomitant of the foreign affairs powers of the Government and outside the confines of the Fourth Amendment.

I would like to conclude. In addition to recognizing a residual right in privacy that is held with third-party data and passing new privacy acts, one of the greatest and least discussed problems, international security infrastructure, is the lack of economic and commercial representation. The National Security Act does not include the Secretary of Treasury as a statutory member. That is done by PPD. Other economic concerns are not represented at a programmatic level of the national security infrastructure. This committee could change that structure to prevent this from happening in the future.

[The prepared statement of Ms. Donohue follows:]

HIGH TECHNOLOGY, CONSUMER PRIVACY, AND U.S. NATIONAL SECURITY

Professor Laura K. Donohue, J.D., Ph.D.*

Written Remarks
Prepared for the U.S. House of Representatives
Committee on Energy and Commerce,
Subcommittee on Commerce, Manufacturing, and Trade
" Cross border Data Flows: Could Foreign Protectionism Hurt U.S. Jobs?"
Sept. 17, 2014

I. INTRODUCTION

Documents released over the past year detailing the National Security Agency's telephony metadata collection program and interception of international content under the Foreign Intelligence Surveillance Act (FISA) directly implicated U.S. high technology companies in government surveillance.[1] The result was an immediate, and detrimental, impact on U.S. firms, the economy, and U.S. national security.

The first Snowden documents, printed June 5, 2013, revealed that the U.S. government had served orders on Verizon, directing the company to turn over telephony metadata under Section 215 of the USA PATRIOT Act.[2] The following day, *The Guardian* published classified slides detailing how the NSA had intercepted international content under Section 702 of the FISA Amendments Act.[3] The type of information obtained ranged from E-mail, video and voice chat, videos, photos, and stored data, to Voice over Internet Protocol, file transfers, video conferencing, notifications of target activity, and online social networking details.[4] The companies

---

* Professor of Law, Georgetown Law and Director, Center on National Security and the Law, Georgetown Law.

[1] *See, e.g.,* Glenn Greenwald and Ewen MacAskill, *NSA Taps into Internet Giants' Systems to Mine User Data, Secret Files Reveal*, THE GUARDIAN (London), June 6, 2013; Barton Gellman and Laura Poitras, *U.S. Intelligence Mining Data from Nine U.S. Internet Companies in Broad Secret Program*, WASH. POST, June 6, 2013; Glenn Greenwald, *NSA collecting Phone Records of Millions of Verizon Customers Daily*, THE GUARDIAN (London), June 6, 2013; Glenn Greenwald, *Microsoft Handed the NSA Access to Encrypted Messages*, THE GUARDIAN, Jul. 11, 2013, *available at* http://www.theguardian.com/world/2013/jul/11/microsoft-nsa-collaboration-user-data; *NSA Taps Yahoo, Google Links*, WASH. POST, Oct. 31, 2013. For statutory and constitutional analysis of the telephony metadata program and the interception of international content, *see* Laura K. Donohue, *Bulk Metadata Collection: Statutory and Constitutional Considerations*, 37(3) HARV. J. OF L. & PUB. POL'Y, 757-900 (2014), *available at* http://scholarship.law.georgetown.edu/cgi/viewcontent.cgi?article=2360&context=facpub; *Section 702 and the collection of International Telephone and Internet Content*, 38(1) HARV. J. OF L. & PUB. POL'Y, (2015), *available at* http://scholarship.law.georgetown.edu/facpub/1355/.

[2] Glenn Greenwald, *NSA Collecting Phone Records of Millions of Verizon Customers Daily*, THE GUARDIAN, June 5, 2013, *available at* http://www.theguardian.com/world/2013/jun/06/nsa-phone-records-verizon-court-order.

[3] Glenn Greenwald and Ewen MacAskill, *NSA Prism Program Taps in to User Data of Apple, Google, and Others*, THE GUARDIAN, June 6, 2013, *available at* http://www.theguardian.com/world/2013/jun/06/us-tech- giants-nsa-data.

[4] *Id.*

involved read like a who's who of U.S. Internet giants: Microsoft, Yahoo, Google, Facebook, PalTalk, YouTube, Skype, AOL, and Apple.[5]

More articles highlighting the extent to which the NSA had become embedded in the U.S. high tech industry followed. In September 2013 ProPublica and the *New York Times* revealed that the NSA had enjoyed considerable success in cracking commonly-used cryptography.[6] The following month the *Washington Post* reported that the NSA, without the consent of the companies involved, had obtained millions of customers' address book data: in one day alone, some 444,743 email addresses from Yahoo, 105,068 from Hotmail, 82,857 from Facebook, 33,697 from Gmail, and 22,881 from other providers.[7] The extent of upstream collection stunned the public – as did slides demonstrating how the NSA had bypassed the companies' encryption, intercepting data as it transferred between the public Internet and the Google cloud.[8]

Further documents suggested that the NSA had helped to promote encryption standards for which it already held the key or whose vulnerabilities the NSA understood but not taken steps to address.[9] Beyond this, press reports indicated that the NSA had at times posed as U.S. companies—without their knowledge—in order to gain access to foreign targets. In November 2013 *Der Spiegel* reported that the NSA and the United Kingdom's Government Communications Headquarters (GCHQ) had created bogus versions of Slashdot and LinkedIn, so that when employees from the telecommunications firm Belgacom tried to access the sites from corporate computers, their requests were diverted to the replica sites that then injected malware into their machines.[10]

As a result of growing public awareness of these programs, U.S. companies have lost revenues, even as non-U.S. firms have benefited.[11] In addition, numerous

---

[5] *Id.*

[6] Nicole Perlroth, Jeff Larson, and Scott Shane, *NSA Able to Foil Basic Safeguards of Privacy on Web*, N. Y. TIMES, Sept. 5, 2013, available at http://www.nytimes.com/2013/09/06/us/nsa-foils-much-internet-encryption.html?pagewanted=all&_r=0.

[7] Barton Gellman and Ashkan Soltani, *NSA Collects Millions of E-mail Address Books Globally*, WASH. POST, Oct. 14, 2013, *available at* http://www.washingtonpost.com/world/national-security/nsa-collects-millions-of-e-mail-address-books-globally/2013/10/14/8e58b5be-34f9-11e3-80c6-7e6dd8d22d8f_story.html.

[8] Barton Gellman and Ashkan Soltani, *NSA Infiltrates Links to Yahoo, Google Data Centers Worldwide, Snowden Documents Say*, WASH. POST, Oct. 30, 2013, *available at* http://www.washingtonpost.com/world/national-security/nsa-infiltrates-links-to-yahoo-google-data-centers-worldwide-snowden-documents-say/2013/10/30/e51d661e-4166-11e3-8b74-d89d714ca4dd_story.html.

[9] James Ball, Julian Borger, and Glenn Greenwald, *Revealed: How US and UK Spy Agencies Defeat Internet Privacy and Security*, THE GUARDIAN, Sept. 5, 2013, *available at* http://www.theguardian.com/world/2013/sep/05/nsa-gchq-encryption-codes-security.

[10] Steven Levy, *How the US Almost Killed the Internet*, WIRED, Jan. 7, 2014, *available at* http://www.wired.com/2014/01/how-the-us-almost-killed-the-internet/all/.

[11] *See, e.g.*, Sam Gustin, *NSA Spying Scandal Could Cost U.S. Tech Giants Billions*, TIME, Dec. 10, 2013, available at http://business.time.com/2013/12/10/nsa-spying-scandal-could-cost-u-s-tech-giants-billions/. ("The National Security Agency spying scandal could cost the top U.S. tech companies billions of dollars over the next several years, according to industry experts. In addition to consumer Internet companies, hardware and cloud-storage giants like IBM, Hewlett-Packard, and Oracle could suffer billions of dollars in losses."); Ellen Messmer, *U.S. High-Tech Industry feeling the Heat from Edward Snowden Leaks*, NETWORKWORLD, Jul. 19, 2013 ("The disclosures about the National Security Agency's massive global surveillance by Edward Snowden, the former information-technology contractor who's now wanted by the U.S. government for treason, is hitting the U.S. high-tech industry hard as it tries to explain its involvement in the NSA data-collection program."); Claire Cain Miller, *Revelations of N.S.A. Spying Cost U.S. Tech Companies*, N. Y. TIMES, Mar. 21, 2014, *available at* http://www.nytimes.com/2014/03/22/business/fallout-from-snowden-hurting-bottom-line-of-tech-companies.html?_r=0 (writing, "Despite the tech companies' assertions that they provide information on

countries, concerned about consumer privacy as well as the penetration of U.S. surveillance efforts in the political sphere, have accelerated localization initiatives, begun restricting U.S. companies' access to local markets, and introduced new privacy protections—with implications for the future of Internet governance and U.S. economic growth. These effects raise attendant concerns about U.S. national security.

Congress has an opportunity to redress the current situation in at least three ways. First, and most importantly, reform of the Foreign Intelligence Surveillance Act would provide for greater restrictions on NSA surveillance. Second, new domestic legislation could extend better protections to consumer privacy. These shifts would allow U.S. industry legitimately to claim a change in circumstance, which would help them to gain competitive ground. Third, the integration of economic concerns at a programmatic level within the national security infrastructure would help to ensure that economic matters remain central to national security determinations in the future.

II. ECONOMIC IMPACT OF NSA PROGRAMS

Billions of dollars are on the line because of worldwide concern that the services provided by U.S. information technology companies are neither secure nor private.[12] Perhaps nowhere is this more apparent than in cloud computing. Approximately 50% of the worldwide revenues previously came from the United States.[13] The domestic market more than tripled in value 2008-2014.[14] But within weeks of the Snowden documents, reports had emerged that U.S. companies such as Dropbox, Amazon Web Services, and Microsoft's Azure were losing business.[15] By December 2013, ten percent of the Cloud Security Alliance had cancelled U.S. cloud services projects as a result of the Snowden information.[16] In January 2014 a survey of Canadian and British businesses found that one quarter of the respondents were moving their data outside the United States.[17] The Information Technology and Innovation Foundation estimates that declining revenues of corporations that focus on cloud computing and data storage alone could reach $35 billion over the next three years.[18] Other commentators, such as Forrester Research analyst James Staten, have put actual losses

---

their customers only when required under law – and not knowingly through a back door – the perception that they enabled the spying program has lingered.")

[12] *IT Industries Set to Lose Billions Because of Privacy Concerns*, UPI, Dec. 17, 2013, available at http://www.upi.com/Business_News/Security-Industry/2013/12/17/IT-industries-set-to-lose-billions-because-of-privacy-concerns/UPI-30251387333206/ ("Information technology companies stand to lose billions of dollars of business because of concerns their services are neither secure nor private.").

[13] *Gartner Predict Cloud computing Spending to Increase by 100% in 2016, Says AppsCare*, PR WEB, July 19, 2012, available at http://www.prweb.com/releases/2012/7/prweb9711167.htm.

[14] *Id.*

[15] David Gilbert, *Companies Turn to Switzerland for Cloud Storage Following NSA Spying Revelations*, INT'L BUSINESS TIMES, July 4, 2013, *available at* http://www.ibtimes.co.uk/business-turns-away-dropbox-towards-switzerland-nsa-486613.

[16] Mieke Eoyang & Gabriel Horwitz, Opinion: *NSA Snooping's Negative Impact on Business Would Have the Foundign Fathers "Aghast,"* FORBES, Dec. 20, 2013, *available at* http://snewsi.com/id/1342616710/NSA-Snoopings-Negative-Impact-On-Business-Would-Have-The-Founding-Fathers-Aghast.

[17] *NSA Scandal: UK and Canadian Business Wary of Storing Data in the US*, PEER 1 HOSTING, Jan. 8, 2014.

[18] *Id. See also* Mary DeRosa, *U.S. Cloud Services Companies Are Paying Dearly for NSA Leaks*, TECH INSIDER, Mar. 24, 2014, *available at* http://www.nextgov.com/voices/mary-derosa/8437/ (reporting estimates of losses of $22 billion over the next three years).

as high as $180 billion by 2016, unless something is done to restore confidence in data held by U.S. companies.[19]

The economic impact of the NSA programs extends beyond cloud computing to the high technology industry. Cisco, Qualcomm, IBM, Microsoft, and Hewlett-Packard have all reported declining sales as a direct result of the NSA programs.[20] Servint, a webhosting company based in Virginia, reported in June 2014 that its international clients had dropped by 50% since the leaks began.[21] Also in June, the German government announced that because of Verizon's complicity in the NSA program, it would end its contract with the company, which had previously provided services to a number of government departments.[22] As a senior analyst at the Information Technology and Innovation Foundation explained, "It's clear to every single tech company that this is affecting their bottom line."[23] The European commissioner for digital affairs, Neelie Kroes, predicts that the fallout for U.S. businesses in the EU alone will amount to billions of Euros.[24]

Not only are U.S. companies losing customers, but they have been forced to spend billions to add encryption features to their services. IBM has invested more than a billion dollars to build data centers in London, Hong Kong, Sydney, and elsewhere, in an effort to reassure consumers outside the United States that their information is protected from U.S. government surveillance.[25] Salesforce.com made a similar announcement in March 2014.[26] Google moved to encrypt terms entered into its browser.[27] And in June 2014 the company released the source code for End-to-End, its newly-developed browser plugin that allows users to encrypt email prior to it being sent across the Internet.[28] The following month Microsoft announced Transport Layer Security for inbound and outbound email, and Perfect Forward Secrecy encryption for access to OneDrive.[29] Together with the establishment of a Transparency Center, where foreign governments could review source code to assure themselves of the integrity of Microsoft software, the company sought to put an end to both NSA back door surveillance and doubt about the integrity of Microsoft products.[30]

---

[19] *IT Industries Set to Lose Billions Because of Privacy Concerns*, UPI, Dec. 17, 2013, available at http://www.upi.com/Business_News/Security-Industry/2013/12/17/IT-industries-set-to-lose-billions-because-of-privacy-concerns/UPI-30251387333206/. This number includes domestic customers who may go elsewhere to find greater privacy protections. *See* Gustin, *supra* note 11.

[20] Sean Gallagher, *NSA Leaks Blamed for Cisco's Falling Sales Overseas*, ARS TECHNICA, Dec. 10, 2013; Paul Taylor, *Cisco Warns Emerging Market Weakness is no Blip*, FIN. TIMES, Dec. 13, 2013; Spencer E. Ante, *Qualcomm CEO Says NSA Fallout Impacting China Business*, WALL. ST. J., Nov. 22, 2013; Miller, *supra* note 11.

[21] Julian Hattem, *Tech Takes Hit from NSA*, THE HILL, June 30, 2014.

[22] Andrea Peterson, *German Government to Drop Verizon over NSA spying Fears*, WASH. POST, June 26, 2014.

[23] *Id.*

[24] Eoyang et al, *supra* note 16.

[25] Miller, *supra* note 11.

[26] *Id.*

[27] Danny Sullivan, *Post-PRISM, Google Confirms Quietly Moving to Make All Searches Secure, Except for Ad Clicks*, SEARCH ENGINE LAND, Sept. 23, 2013, *available at* http://searchengineland.com/post-prism-google-secure-searches-172487.

[28] Klint Finley, *Google Renews Battle With the NSA by Open Sourcing Email Encryption Tool*, WIRED, June 3, 2014, *available at* http://www.wired.com/2014/06/end-to-end/.

[29] Matt Thomlinson, Vice President Trustworthy Computing Security, Microsoft, *Advancing our Encryption and Transparency Efforts*, Press Release, *available at* http://blogs.microsoft.com/on-the-issues/2014/07/01/advancing-our-encryption-and-transparency-efforts/. *See also* Carly Page, *Microsoft Installs Tougher Outlook and Onedrive Encryption to Curb NSA Snooping*, THE INQUIRER, Jul. 1, 2014, *a* http://www.theinquirer.net/inquirer/news/2353073/microsoft-installs-better-outlook-and-onedrive-encryption-to-curb-nsa-snooping.

[30] *Id.*

Foreign technology companies, in turn, are seeing revenues increase.[31] Runbox, for instance, an email service based in Norway and a direct competitor to Gmail and Yahoo, almost immediately made it publicly clear that it does not comply with foreign court requests for its customers' personal information.[32] Its customer base increased 34% in the aftermath of the Snowden revelations.[33] Mateo Meier, CEO of Artmotion (Switzerland's biggest offshore data hosting company), reported that within the first month of the Snowden releases, the company saw a 45% rise in revenue.[34] Because Switzerland is not a member of the EU, the only way to access data in a Swiss data center is as a result of an official court order demonstrating guilt or liability; there are no exceptions for the United States.[35] In April 2014, Brazil and the European Union, which previously used U.S. firms to supply undersea cables for transoceanic communications, decided to build their own cables between Brazil and Portugal, using Spanish and Brazilian companies in the process.[36] OpenText, Canada's largest software company, now guarantees customers that their data remains outside the United States. Deutsche Telekom, a cloud computing provider, is similarly gaining more customers.[37] In sum, numerous foreign companies are marketing their products as "NSA proof" or "safer alternatives" to those offered by U.S. firms, gaining market share in the process.[38]

III. FOREIGN GOVERNMENT RESPONSES

The Snowden documents revealed not just the extent to which high technology companies had become coopted, but that the targets of NSA surveillance include both allied and non-allied countries.[39] The resulting backlash has led some commentators to raise concern that "the Internet will never be the same."[40] Jurisdictional questions and national borders previously marked the worldwide Internet discussions.[41] Countries, however, are now using the disclosures to restrict data storage to national borders, making it more difficult for the United States to gain access.[42] As risk is the balkanization of the Internet, undermining its traditional culture of open access, and increasing the cost of doing business.[43]

---

[31] *Id.*
[32] Miller, *supra* note 11.
[33] *Id.*
[34] Gilbert, *supra* note 15.
[35] *Id.*
[36] Miller, *supra* note 11.
[37] *Id.*
[38] Mark Scott, *European Firms Turn Privacy into Sales Pitch*, N. Y. TIMES, June 11, 2014.
[39] *See, e.g.*, Laura Poitras, Marcel Rosenbach, Fidelius Schmid and Holger Stark, *NSA Spied on European Union Offices*, DER SPIEGEL, June 29, 2013; Laura Poitras, Marcel Rosenbach, and Holger Stark, *Codename "Apalachee": How America Spies on Europe and the UN*, DER SPEIGEL ONLINE, Aug. 26, 2013, *available at* http://www.spiegel.de/international/world/secret-nsa-documents-show-how-the-us-spies-on-europe-and-the-un-a-918625.html; *EXCUSIVE: US spies on Chinese Mobile Phone Companies, Steals SMS Data: Edward Snowden*, SOUTH CHINA MORNING POST, June 22, 2013, *available at* http://www.scmp.com/news/china/article/1266821/us-hacks-chinese-mobile-phone-companies-steals-sms-data-edward-snowden; Lana Lam, *US Hacked Pacnet, Asia Pacific Fibre-Optic Network Operator, in 2009*, SOUTH CHINA MORNING POST (HONG KONG), June 23, 2013; Ewen MacAskill, Julian Borger, NEW NSA LEAKS SHOW HOW US IS BUGGING ITS EUROPEAN ALLIES, THE GUARDIAN (LONDON), June 30, 2013.
[40] Levy, *supra* note 10.
[41] *See, e.g.*, Kristina Irion, *Government Cloud Computing and National Data Sovereignty*, SOCIAL SCIENCE RESEARCH NETWORK, June 2012.
[42] Levy, *supra* note 10.
[43] *Id.*

A. Data Localization and Data Protection

Countries around the world are increasingly adopting data localization laws, restricting the storage, analysis, and transfer of digital information to national borders.[44] To some extent, the use of barriers to trade as a means of incubating tech-based industries predated the Snowden releases.[45] However, in the aftermath of the leaks, the dialogue has accelerated. The asserted purpose is to protect both government data and consumer privacy.

As of the time of writing, China, Greece, Malaysia, Russia, South Korea, Venezuela, Vietnam, and others have already implemented local data server requirements.[46] Turkey has introduced new privacy regulations preventing the transfer of personal data (particularly locational data) overseas.[47] Others, such as Argentina, India, and Indonesia are actively considering new laws, even as Brazilian president, Dilma Rousseff, has been promoting a law that would require citizens' personal data to be stored within domestic bounds.[48] Germany and France are considering a Schengen routing system, retaining as much online data in the European Union as possible.[49]

As a regional matter, the EU Commission's Vice President, Viviane Reding, is pushing for Europe to adopt more expansive privacy laws.[50] And in March 2014 the European Parliament passed the Data Protection Regulation and Directive, imposing strict limits on the handling of EU citizens' data. Regardless of where the information is based, those handling the data must obtain the consent of the data subjects to having their personal information processed. They also retain the right to later withdraw consent. Those violating the directive face steep fines, including up to five percent of revenues.

In addition, the Civil Liberties, Justice, and Home Affairs Committee of the European Parliament passed a resolution calling for the end of the US/EU Safe Harbor agreement.[51] Some 3000 U.S. companies rely on this framework to conduct business with the EU.[52]

---

[44] Jonah Force Hill, *The Growth of Data Localization Post-Snowden: Analysis and Recommendations for U.S. Policymakers and Industry Leaders*, 2(3) LAWFARE RESEARCH PAPER SERIES, Jul. 21, 2014.

[45] *See, e.g.*, Stephen J. Ezell, Robert D. Atkinson, and Michaelle A. Wein, *Localization Barriers to Trade: Threat to the Global Innovation Economy, The Information Technology & Innovation Foundation*, Sept. 2013, *available at* http://copyrightalliance.org/sites/default/files/resources/2013-localization-barriers-to-trade.pdf.

[46] Sidley Austin, LLP., *Privacy, Data Security and Information Law Update*, Dec. 30, 2013, available at http://www.sidley.com/files/News/1ce5014c-9236-41cb-87ba-32dee9163fed/Presentation/NewsAttachment/6d72f3e3-6b28-4d23-bc9a-5493071c9b13/12.30.2013%20Privacy%20Update.pdf.

[47] Richard Chirgwin, *USA Opposes "Schengen Cloud" Eurocentric Routing Plan*, THE REGISTER (United Kingdom), Apr. 7, 2014, *available at* http://www.theregister.co.uk/2014/04/07/keeping_data_away_from_the_us_not_on_ustr/.

[48] Levy, *supra* note 10.

[49] *See, e.g., Weighing a Schengen Zone for Europe's Internet Data*, DEUTSCHE WELL, Feb. 20, 2014, *available at* http://www.dw.de/weighing-a-schengen-zone-for-europes-internet-data/a-17443482 ; *Deutsche Telekom: "Internet Data Made in Germany should Stay in Germany,"* DEUTSCHE WELLE, Oct. 18, 2013, *available at* http://www.dw.de/about-dw/who-we-are/s-3325.

[50] Mike Eoyang & Gabriel Horwitz, *Opinion: NSA Snooping's Negative Impact on Business Would have the Founding Fathers "Aghast,"* FORBES, Dec. 20, 2013.

[51] *NSA Snooping; MEPs TABLE PROPOSALS TO PROTECT EU CITIZENS' PRIVACY*, EUROPEAN PARLIAMENT, Feb. 12, 2014.

[52] Alex Byers, *Tech Safe Harbor Under Fire in Europe*, POLITICO MORNING TECH, Nov. 6, 2013.

In May 2014 the EU Court of Justice ruled that users have a "right to be forgotten" in their use of online search engines. The case derived from a complaint lodged against a Spanish newspaper, as well as Google Spain and Google Inc., claiming that notice of the plaintiff's repossessed home on Google's search engine infringed his right to privacy because the incident had been fully addressed years before. He requested that the newspaper be required to remove or alter the pages in question to excise data related to him, and that Google Spain or Google Inc. be required to remove the information. The EU court found that even where the physical server of a company processing information is not located in Europe, as long as the company has a branch or subsidiary and is doing business in a Member state, the 1995 Data Protection Directive applies.[53] Because search engines contain personal data, they are subject to such data protection laws. The Court recognized that, under certain conditions, individuals have the "right to be forgotten"—i.e., the right to request that search engines remove links containing personal information. Data that is inaccurate, inadequate, irrelevant, or excessive may be removed. Not absolute, the right to be forgotten must be weighed against competing rights, such as freedom of expression and the media.

Various country-specific privacy laws are similarly poised to be introduced. Their potential economic impact is not insubstantial: the Information Technology and Innovation Fund estimates that data privacy rules could retard the growth of the technology industry by up to four percent, impacting U.S. companies' ability to expand and forcing them out of existing markets.[54]

The current dialogue is merely the latest in a series of growing concerns about the absent of effective privacy protections within the U.S. legal regime. High tech companies appear to see this as a potential step forward. As Representative Justin Amash (MI-R), has explained, "Businesses increasingly recognize that our government's out-of-control surveillance hurts their bottom line and costs American jobs. It violates the privacy of their customers and it erodes American businesses' competitive edge."[55]

It is with concern about the impact of lack of privacy controls on U.S. competitiveness in mind that in December 2013 some of the largest U.S. Internet companies launched a campaign to pressure the government to reform the NSA surveillance programs. Microsoft General Counsel Brad Smith explained: "People won't use technology they don't trust." He added, "Governments have put this trust at risk, and governments need to help restore it." Numerous high technology CEOs supported the initiative, such Google's Larry Page, Yahoo's Marissa Mayer, and Facebook's Mark Zuckerberg.[56] The aim is to limit government authority to collect user data, to institute better oversight and accountability, to ensure greater transparency about what the government is requesting (and obtaining), to increase respect for the free flow of data across borders, and to avoid political clashes on a global scale. Mayer, explained, "Recent revelations about government surveillance activities have shaken the trust of our users, and it is time for the United States government to act to restore the confidence of citizens around the world."[57]

---

[53] Directive 95/46/EC of the European Parliament and of the Council of 24 Oct. 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data.
[54] Michael Hickens, AMERICAN SPYING STYMIES TECH FIRMS, WALL STREET J., Feb. 18, 2014.
[55] Gustin, *supra* note 11
[56] *Id.*
[57] *Id.*

B. Global Initiatives Regarding Internet Governance

Apart from economic considerations, the backlash raises question about the future of Internet governance. From the inception of the Internet, the U.S.-based Internet Corporation for Assigned Names and Numbers (ICANN) has governed the web. As time has progressed, and the Internet has become part of the global infrastructure, there have been calls from several nations to end U.S. dominance and to have the International Telecommunication Union (ITU), an entity within the UN, become the governing body. The revelations have not only contributed further to such calls, but they have spurred increased discussion of the need for regional Internet control.

Over the past decade, three main groups have emerged to vie for control of the Internet. The first is centered on states, who consider the question in light of national sovereignty. It is comprised of developing countries as well as large, emerging economies like China, Russia, Brazil, and South Africa.[58] It overlaps significantly with the Group of 77 (consisting of more than 100 countries which emerged from the non-aligned movement in the Cold War). These states are critical of the United States and its dominant role in Internet governance and oppose private sector preeminence, on the grounds that they are pawns of the United States. Emphasis instead is placed on the UN and the ITU as potential repositories of Internet authority.

The second group is civil society. The third is the private sector. These groups both tend to support what is referred to as a "multistakeholder model:" i.e., native Internet governance institutions that are generally nonprofit entities in the private sector.[59] Membership includes both technical experts (e.g., ICANN and Regional Internet Registries), as well as multinational corporations (e.g., Microsoft, Facebook, and AT&T). Prior to the Snowden releases, Japan, the EU, and the US found themselves in this camp. Civil society organizations emphasize Internet freedom, consumer privacy, and user rights—often bringing them into conflict with the states who comprise the G77-type group.[60]

As one commentator explains, "This alignment of actors has been in place since the 2003 World Summit on the Information Society (WSIS) meetings. But the Snowden NSA revelations seem to have destabilized this settled political alignment."[61]

In brief, ICANN and Brazil have formed an alliance, condemning U.S. actions. Concern about the latest revelations spurred a major conference in April 2014: i.e., the *Global Multistakeholder Conference on the Future of Internet Governance*. The purpose of the meeting, which was held in Sao Paulo, was "to produce universal internet principles and an institutional framework for multistakeholder Internet governance."[62]

It is not clear how the newest shifts will be resolved—either temporarily or in the future. But significant, and enormously important, questions have been raised by the Snowden revelations: How should the Internet governance be structured to ensure legitimacy and compliance? Who gets to make the decision about what such governance looks like? Which bodies have the authority to establish future rules and procedures? How are such bodies constituted and who selects their membership?

---

[58] Milton Mueller and Ben Wagner, *Finding a Formula for Brazil: Representation and Legitimacy in Internet Governance*, (2013), p. 3, *available at* http://www.internetgovernance.org/wordpress/wp-content/uploads/MiltonBenWPdraft_Final.pdf.
[59] *Id.*
[60] *Id.*
[61] *Id.*, at 4.
[62] *Id.*, at 1.

These questions are fundamentally at odds with the decentralization tendencies in the Internet—tendencies that have been exaggerated post-Snowden as a result of regional efforts to expand the local sphere of influence and to protect consumer and state privacy from U.S. surveillance.

The U.S. government's failure to address the situation domestically has undermined the tech industry. Despite calls from the companies for legislative reform to address the breadth of the NSA programs,[63] there has been no significant shift that would allow companies to approach their customers to say, with truth, that the situation has changed. Resultantly, American companies are losing not just customers, but the opportunity to submit proposals for contracts for which they previously would have been allowed to compete.[64] And the future of Internet governance hangs in the balance.

IV. ECONOMIC SECURITY AS NATIONAL SECURITY

The NSA programs illustrate lawmakers' failure to recognize the degree to which economic strength is central to national security, as well as the importance of the high technology industry to the U.S. economy. The concept of economic security as national security is not new: the Framers and the generations that followed acknowledged the importance of economic strength as central to national security. Our more recent understandings, however, have gotten away from the concept, in the process cleaving important interests out of the calculations required to accurately understand the implications of government actions. Unintended consequences have resulted: the NSA revelations, for instance, may have driven bad actors to seek non-U.S. companies for ISP services, creating gaps in insight into their operations. They have also undermined U.S. efforts to call other countries to heel for their exploitation of international communications to gain advantages over U.S. industry. In sum, the expansive nature of the programs may well have acted to undermine U.S. national security in myriad ways linked to the country's economic interests.

A. Economic Security from the Founding

Despite its appearance throughout U.S. history, the term "national security" is rarely defined.[65] The 1947 National Security Act, for instance, which, *inter alia*, constituted the National Military Establishment (later the Department of Defense), and the National Security Council, refers to "national security" more than 100 times; yet it does not define the term.[66] The Foreign Intelligence Surveillance Act of 1978 employs the term nearly a dozen times, to ascertain what matters fall within the Foreign Intelligence Surveillance Court's (FISC) purview, who can certify an application to FISC, and under what conditions *in camera* and *ex parte* proceedings can be held.[67] Where the Attorney General ascertains that a national security threat exists, officials may secretly search and seize property—waiting notice otherwise required under the Fourth Amendment.[68] But no definition is provided in FISA. Nor

---

[63] *See, e.g.*, Gustin, *supra* note 11 (reporting that the nation's largest Internet companies are calling for Congress and the Administration to reform the secret surveillance programs).
[64] Miller, *supra* note 11.
[65] *See* Laura K. Donohue, *The Limits of National Security*, 48 AM. CRIM. L. REV., 1579 (2011).
[66] National Security Act of 1947, Pub. L. No. 80-235, 61 Stat. 495 (current version at 50 U.S.C. §401 (2006)).
[67] 50 U.S.C. §§1803(e), 1804(a), 1806(f), and 1845(f).
[68] 50 USC §1825(b).

does the USA PATRIOT Act prove more illuminating—despite referring to national security more than two dozen times.[69]

Where we do find definitions in the U.S. Code, they tend to limit consideration to foreign affairs and matters related to military strength. Thus, under the Classified Information Procedures Act, "national security" is understood as involving matters related to the "national defense and foreign relations of the United States."[70] Nowhere does the definition reference U.S. economic security.

In the amended National Security Act, while the term could potentially be understood to encompass U.S. economic security, the actual definition does not specify a precise link to economic vitality. Instead, "intelligence related to national security" refers to:

> all intelligence, regardless of the source from which derived and including information gathered within or outside the United States, that
> (A) pertains, as determined consistent with any guidance issued by the President, to more than one United States Government agency; and
> (B) that involves—
> (i) threats to the United States, its people, property, or interests;
> (ii) the development, proliferation, or use of weapons of mass destruction; or
> (iii) any other matter bearing on United States national or homeland security.[71]

The Federal Information Security management Act of 2002 (providing rules for government-wide information security) similarly fails to consider the economic underpinnings of national security, instead, understanding national security systems as any system:

> (i) the function, operation, or use of which
> (I) involves intelligence activities;
> (II) involves cryptologic activities related to national security;
> (III) involves command and control of military forces;
> (IV) involves equipment that is an integral part of a weapon or weapons system; or
> (V) subject to subparagraph (B), is critical to the direct fulfillment of military or intelligence missions; or
> (ii) is protected at all times by procedures established for information that have been specifically authorized under criteria established by an Executive order or an Act of Congress to be kept classified in the interest of national defense or foreign policy.[72]

While there may be room in the definition for economic considerations, they are not front and center.

Executive Branch articulations prove little better. President George W. Bush's five-page National Security Presidential Directive 1 referred to "national security"

---

[69] *See, e.g.*, Pub. L. No. 107-56, §505.
[70] Classified Information Procedures Act §1(b), 18 U.S.C. app. 3 (2006).
[71] 50 U.S.C.A. § 401a(5) (2012).
[72] Federal Information Security Management Act of 2002, Pub. L. 107-347, § 201, 116 Stat. 2947 (2002) (codified at 44 U.S.C. § 3542(b)(2)(A)).

thirty-three times, without any definition.[73] President Barak Obama's Presidential Policy Directive 1 (PPD-1), in turn, addressing the National Security Council, referred to "national security" thirty-three times—without ever defining it.[74] And like the Executive Branch, Courts tend to look to the military and diplomatic aspects of national security, instead of their economic concomitant.[75]

Despite the lack of emphasis on economic strength, the Founders were well aware of the importance of the economy in fostering international independence. The Articles of Confederation failed in significant part because the national government lacked the resources, and the country the economic strength, to protect the Union. For Alexander Hamilton, absent military might, diplomatic stature, and commercial success, the country would cease to exist.[76]

One of the first expansions of the executive, accordingly, was to include a Secretary of the Treasury, which, along with the Secretary of War and the establishment of the office of Attorney General, reflected the purposes for which Union had been sought: foreign relations, military strength, economic growth, and the rule of law. In his *Farewell Address*, President George Washington called for U.S. energies to be directed towards strengthening the U.S. economy: "[T]he great rule of conduct for us in regard to foreign nations is in extending our commercial relations, to have with them as little political connection as possible."[77]

The federal government was willing, from a very early date, to act in support of its commercial interests with whatever diplomatic, legal, and military power it could muster.[78] The Monroe Doctrine was premised largely on this approach. In 1837 President Martin Van Buren came to office determined to continue Washington's legacy, underscoring the importance of avoiding entangling alliances while pursuing America's economic interests abroad.[79] President Zachary Taylor came to office in 1849 determined to continue the course, emphasizing the importance of bolstering trade as a means of securing the country.[80] The 1950 Clayton-Bulwer Treaty ensured that future canal access through Central America would be open to international trade.[81] As Millard Fillmore succeeded Taylor, he considered commerce central to U.S. interests abroad—for this reason, the Navy would require further resources to protect trade along the Pacific Coast.[82] Upon taking office, President Franklin Pierce reiterated the same policies: of the complicated European tumults and anxieties, the

---

[73] George W. Bush, NSPD-1, National Security Presidential Directive 1: Organization of the National Security Council System (2001).

[74] *See* Barack Obama, PSD-1, Presidential Study Directive 1: Organizing for Homeland Security and Counterterrorism 1-2 (2009), *available at* http://www.fas.org/irp/offdocs/psd/psd-1.pdf ("[C]onceptually and functionally, [national security and homeland security] should be thought of together rather than separately.").

[75] *See, e.g., See N.Y. Times Co.*, 403 U.S. at 719 (Black, J., concurring).

[76] FEDERALIST No. 1, (Alexander Hamilton).

[77] President George Washington, Farewell Address to the People of the United States (Sept. 19, 1796), *reprinted in* S. Doc. No. 106-21, at 6 (2d Sess. 2000) [hereinafter Washington, Farewell Address], http://www. access.gpo.gov/congress/senate/farewell/sd106-21.pdf.

[78] For a catalog of every military intervention in support of U.S. commercial interests, *see* WILLIAM APPLEMAN WILLIAMS, EMPIRE AS A WAY OF LIFE: AN ESSAY ON THE CAUSES AND CHARACTER OF AMERICA'S PRESENT PREDICAMENT ALONG WITH A FEW THOUGHTS ABOUT AN ALTERNATIVE (1st ed. 1980).

[79] President Martin Van Buren, Inaugural Address (Mar. 4, 1837).

[80] President Zachary Taylor, Inaugural Address (Mar. 5, 1849).

[81] Convention Between the United States of America and Her Britannic Majesty (Clayton-Bulwer Treaty), U.S.-Gr. Brit., Apr. 19, 1850, 9 Stat. 995.

[82] President Millard Fillmore, First Annual Message to Congress (Dec. 2, 1850), *available at* http://www.presidency.ucsb.edu/ws/index.php?pid=29491&st=fillmore&st1=#axzz1Wo2idoeG.

United States was to be exempt, "But the vast interests of commerce are common to all mankind, and the advantages of trade and international intercourse must always present a noble field for the moral influence of a great people." The United States went on to emphasize its dealings with Asia and to sign an historic trade agreement with Japan.[83] Expansionism, and the economic benefits it brought, similarly proved central to U.S. national security. "Should [new possessions] be obtained," Pierce asserted during his *Inaugural Address*, "it will be through no grasping spirit, *but with a view to obvious national interest and security*, and in a manner entirely consistent with the strictest observance of national faith." From the 1898 Spanish-American War forward, the country promoted its national interests through formative political, military, and economic engagement in the international arena.

2. National Security Infrastructure

The National Security Council (NSC) is "the principal forum for consideration of national security policy issues requiring Presidential determination."[84] The President looks to the forum for advice and assistance in matters ranging from domestic, foreign and military, to intelligence and economic.[85] It is thus somewhat surprising that the 1947 National Security Act includes neither the Secretary of the Treasury, nor the Secretary of Commerce, as permanent (statutory) members of the NSC.

Instead, the entity is chaired by the President, with formal membership extended to the Vice President, the Secretary of State, and the Secretary of Defense. The Chair of the Joint Chiefs of Staff acts as the statutory military advisor, the Director of National Intelligence the statutory intelligence advisor, and the Director of National Drug Control Policy as the statutory drug control policy advisor.

Under PDD-1, the NSC includes the Secretary of Treasury, and "When international economic issues are on the agenda of the NSC, the NSC's regular attendees will include the Secretary of Commerce, the United States Trade Representative, the Assistant to the President for Economic Policy, and the Chair of the Council of Economic Advisers."[86]

When the emphasis, however, is not international economic issues, the structure does not cement economic concerns into the discussion. Nor does it contemplate the inclusion of Treasury or Commerce as an operational matter—i.e., when the intelligence community is deciding whether to develop a surveillance program. Such matters are not brought directly to the NSC.[87]

To the extent that the failure to include these members at the most basic level reflects a perspective that potentially sidelines economic concerns, the continued failure to build in strong representation at a programmatic level underscores the concern. Economic concerns may be treated with seriousness, but they are not meaningfully integrated into the national security infrastructure.

3. Unintended Consequences

There are various ways in which the failure to fully take account of the impact of the programs on U.S. industry may have acted to undermine U.S. security beyond weakening the economy. The revelations, for instance, may well have driven enemies

[83] Treaty of Amity and Commerce, U.S.-Japan, July 29, 1858, 12 Stat. 1051.
[84] PPD-1, *Organization of the National Security Council System*, Feb. 13, 2009.
[85] *Id.*
[86] PDD-1, at 2.
[87] DeRosa, *supra* note 18.

of the United States to use other countries' Internet Service Providers, thus creating a gap in our insight into their operations. They may similarly spur the initiation of encryption techniques that the NSA will have no means to address—making the country less secure because of the perceived overreach of the agency. The revelations have also undermined U.S. credibility in challenging other countries' efforts to obtain trade secrets and other information through state surveillance. China provides one of the strongest examples.

Online warfare between China and the United States has simmered in the background, until in early 2013 the Obama Administration began to make it center stage. In January 2013 the *New York Times* reported that Chinese hackers had infiltrated its computers following a threat that if the paper insisted on publishing a story about its prime minister, consequences would follow.[88] The following month a security firm, Mandiant, revealed that the Chinese military unit 61398 had stolen data from U.S. companies and agencies.[89] In March 2013 President Obama's national security advisor publicly urged China to reduce its surveillance efforts—following which classified documents leaked to the public demonstrated the extent to which China had infiltrated U.S. government servers.[90] In May 2013 the National Security Advisor flew to China to lay the groundwork for a summit, in which cyber surveillance would prove center stage.[91] Two days before the Obama-Xi meeting was scheduled to take place, *The Guardian* ran the first story on the NSA programs.[92] On June 7, when Obama raised the question of Chinese espionage, Xi responded by quoting the Guardian and suggesting that the U.S. should not be lecturing the Chinese about surveillance.[93]

Although differences may mark the two countries approaches to surveillance (e.g., in one case for economic advantage, in the other for political or security advantage), the broader translation for the global community has been one in which the United States has lost high ground to try to restrict cybersurveillance by other countries.

V. STEPS REQUIRED TO REDRESS THE CURRENT SITUATION

Numerous steps could be taken by Congress to address the situation in which U.S. industry currently finds itself. The most effective and influential decision that legislators could take would be to curb the NSA's authorities under the Foreign Intelligence Surveillance Act. This action has two components: first, ending the telephony metadata collection program and, second, restricting the use of to/from, or about collection under upstream interceptions. Both programs would further benefit from greater transparency, to make it clear that their aim is to prevent foreign aggression and to prevent threats to U.S. national security—not to engage in the interception of trade secrets or to build dossiers on other countries' populations.

The second most effective change that could be undertaken would be to introduce stricter privacy controls on U.S. companies, in the process bringing the United States into closer line with the principles that dominate in the European Union. The two entities are not as far apart as the dialogue might have one assume, and so changes required in this sphere would be minimal. Together, these two alterations—curbing the NSA surveillance programs and providing increased consumer protections for

---

[88] Kurt Eichenwald, *How Edward Snowden Escalated Cyber War*, NEWSWEEK, Nov. 1, 2013.
[89] *Id.*
[90] *Id.*
[91] *Id.*
[92] *Id.*
[93] *Id.*

privacy—would allow U.S. industry to argue changed circumstance to allow companies to again become competitive for contracts and markets to which they seek access.

A third alteration that would make a substantial difference over the longer term relates to the national security infrastructure. The current failure of the United States to integrate economic concerns creates a vulnerability for the country in terms of the breadth and depth of programs subsequently adopted. New thought needs to be given to how to take on board—and mitigate—potentially devastating economic consequences of government surveillance efforts.

A. FISA Alterations

In addition to the economic impact of NSA telephony metadata collection (discussed, *infra*), the program runs contrary to Congressional intent in introducing the Foreign Intelligence Surveillance Act, contradicts the statutory language, and violates the Fourth Amendment.[94] In 2014 the Privacy and Civil Liberties Oversight Board came to a similar conclusion,[95] as did the President's own appointed Review Group, charged with considering the telephony metadata collection program, in 2013.[96]

Accordingly, the President announced on January 17, 2014 that he was "ordering a transition that will end the Section 215 bulk metadata program as it currently exists, and establish a mechanism that preserves the capabilities we need without the government holding this bulk metadata."[97] The alternative approach was to be developed by March 28, 2014. Nine months later, on September 13, 2014, the Foreign Intelligence Surveillance Court approved DOJ's request to extend the program for another 90 days—without any transition program in place.

Although the President issued a new presidential directive in January 2014 for U.S. signals intelligence activities both at home and abroad, the classified nature of parts of the document, international skepticism about the Administration's commitment to privacy, and the failure of the Administration to make good on its promise of transition to a new program meant that the global community, with good reason, has questioned whether anything has really changed. No new legislation is in place that would provide limits on the Executive Branch beyond those that operated for the duration of the bulk collection program.

As a matter of Section 702 and the interception of international content, both PRISM and upstream collection present global concerns—neither of which have been addressed through any legislative change. The existence of these programs, while perhaps statutorily consistent with the FISA Amendments Act, as well as constitutionally sufficient with regard to the interception of non-U.S. persons

---

[94] Laura K. Donohue, *Bulk Metadata Collection: Statutory and Constitutional Considerations*, 37(3) HARV. J. OF L. & PUB. POL'Y, 757-900 (2014), *available at* http://scholarship.law.georgetown.edu/cgi/viewcontent.cgi?article=2360&context=facpub

[95] PRIVACY AND CIVIL LIBERTIES OVERSIGHT BOARD, REPORT ON THE TELEPHONE RECORDS PROGRAM CONDUCTED UNDER SECTION 215 OF THE USA PATRIOT ACT AND ON THE OPERATIONS OF THE FOREIGN INTELLIGENCE SURVEILLANCE COURT, Jan. 23, 2014, *available at* https://www.eff.org/files/2014/01/23/final_report_1-23-14.pdf.

[96] PRESIDENT'S REVIEW GROUP, LIBERTY AND SECURITY IN A CHANGING WORLD: REPORT AND RECOMMENDATIONS OF THE PRESIDENT'S REVIEW GROUP ON INTELLIGENCE AND COMMUNICATIONS TECHNOLOGIES, Dec. 12, 2013, available at http://apps.washingtonpost.com/g/page/world/nsa-review-boards-report/674/.

[97] *Remarks by the President on Review of Signals Intelligence*, Jan. 17, 2014, *available at* http://www.whitehouse.gov/the-press-office/2014/01/17/remarks-president-review-signals-intelligence.

communications, where the individual is reasonably believed to be located outside the United States, as a policy matter, goes some way towards undermining international confidence in U.S. companies.

The Fourth Amendment does not reach non-U.S. persons based overseas who lack a substantial connection to the United States.[98] Writing for the Court in *United States v. Verdugo-Urquidez*, Chief Justice Rehnquist concluded that "the people" referred to in the Fourth Amendment indicate a particular group—not merely people *qua* people.[99] His reading stems from a deeply Aristotelian approach: i.e., one that emphasizes membership in the polis (πόλις), or political community, as a concomitant of forming a structure of government.[100] As members of the polis, U.S. persons, both distributively and collectively, obtain the protections of the constitution.

Looked at in this regard, the Constitution itself embodies the collective organization of "the people" into one entity. "U.S. persons" and "the people" are therefore one and the same. The "right of the people" thus refers to a collective group of individuals "who are part of a national community or who have otherwise developed sufficient connection with this country to be considered part of that community."[101]

Very few cases address precisely what constitutes sufficient contact with the United States to satisfy the "substantial connections" aspect of the majority's decision. Those that do point in seemingly different directions.[102] At a minimum, however, it would be extraordinary to assume that simply because an individual uses a U.S. company, he or she thereby gains the protections of the Fourth Amendment. This was the basic argument underlying the "modernization" of FISA in the first place, to take account of bad actors, communicating overseas, who would suddenly fall within the more protective FISA regime merely because their communications happened to come within U.S. territory by nature of the carrier in question.

Even recognizing, however, that few constitutional barriers may apply to the programmatic use of Section 702 insofar as it is applied to non-U.S. persons (leaving aside the questions that accompany the incidental collection of U.S. persons' information, as well as entirely domestic conversations), as a matter of policy, certainly both PRISM and the use of to/from or about collection in upstream gathering has dramatically undermined U.S. industry. As a matter of policy, therefore, greater restrictions, more transparency, and more effective oversight of the international collection of content may help to alter the situation with regard to the skepticism expressed towards U.S. companies.

B. Privacy Law Harmonization

Much ink has been spilled on the cultural and practical differences between the U.S. and EU with regard to data protection and privacy law. These differences have been over-blown.

---

[98] *Section 702 and the collection of International Telephone and Internet Content*, 38(1) HARV. J. OF L. & PUB. POL'Y, (2015), *available at* http://scholarship.law.georgetown.edu/facpub/1355/.

[99] United States v. Verdugo-Urquidez, 494 U.S. 259, 265 (1990) (per curiam).

[100] ARISTOTLE, POLITICS, BOOK I (350 BC), trans. by Benjamin Jowett, *available at* http://classics.mit.edu/Aristotle/politics.1.one.html; also *available at* http://www.perseus.tufts.edu/hopper/text;jsessionid=91A85450747C74DF609D266E0A8DF8E5?doc=Perseus%3atext%3a1999.01.0057 (in the original Greek).

[101] 494 U.S. at 265 (per curiam).

[102] Orin Kerr, *The Fourth Amendment and the Global Internet*, 67 STAN. L. REV. (forthcoming 2015), at 8-9.

There are myriad ways in which the two regions reflect a similar approach. Just as the United States' Fourth Amendment protects the right to privacy, for instance, Article 8 of the European Convention for the Protection of Human Rights and Fundamental Freedoms embraces the same.[103] These documents constitutionally ground two fundamental liberty interests in the respective regions' governing frameworks: (a) the right to privacy, and (b) freedom from arbitrary invasion of one's private sphere. In the European Union, these liberties are supported by EU-wide directives, such as the 1995 European Data Protection Directive and the EU Internet Privacy Law of 2002. Further, in both the EU and the U.S. such liberty interests are protected through national legislation, in which a judicial remedy is provided for a breach of the right to privacy.[104] The manner in which these rights are treated is similarly consistent. In both spheres, these rights are offset against the obligations owed by the data holder to the individual to whom the information relates.[105]

As a substantive matter, the two regions have adopted similar provisions. In both the EU and the U.S., for instance, heightened protections are provided for what is known as personally-identifiable information.[106] A series of exceptions to the dominant structure is provided in two central areas: security (including, e.g., criminal law, public security, defense, and national security) and freedom of expression (such as with regard to journalism, literary pursuits, artistic expression, and political opinions).[107] To ensure that the substantive measures reflect the underlying constitutional principles, both regions insist on minimization—i.e., that the information collected on individuals be limited to what is strictly necessary for the purposes delineated by statute.[108]

Both the U.S. and the EU have established a set of substantive requirements related to individuals' knowledge that data about them is being collected, stored, and possibly shared with others. Consent, for instance, is central to both systems.[109] Much has been made in regard to the distinction between the opt-in (European approach) versus the opt-out (American approach). What has been lost, however, is that both approaches rely on the consent of the subject (subject to specific exceptions, above), in order to proceed with data gathering, analysis, and distribution. To

---

[103] *Compare* "The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized." U.S. CONST., 4th Amend., and "Everyone has the right to respect for his private and family life, his home and his correspondence." Eur. Conv. H.R. & F. F., Art. 8.

[104] *Compare* EU Directive 95/46/EC of the European Parliament and of the Council of 24 Oct. 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, Recitations No. 55 [hereinafter 1995 EU Directive], and U.S. statutory provisions related to privacy (including, *inter alia*: the Americans with Disabilities Act, the Cable Communications Policy Act of 1984, the Children's Internet Protection Act of 2001, Children's Online Privacy Protection Act of 1998, Fair Credit Reporting Act, Driver's Privacy Protection Act of 1994, Electronic Communications Privacy Act of 1986, Gramm-Leach-Bliley Financial Services Modernization Act of 1999, Privacy Act of 1974, Privacy Protection Act of 1980, Right to Financial Privacy Act of 1978, Telephone Consumer Protection Act of 1991, Video Privacy Protection Act of 1988, and the Health Insurance Portability and Accountability Act of 1996, Pub. L. 104-191, 110 Stat. 1936, Aug. 21, 1996).

[105] *Compare* 1995 EU Directive, Recitation No. 25, and U.S. laws, *supra* note 5.

[106] *Compare, e.g.,* 1995 EU Directive, Recitation No. 26, and the Systems of Records Notice requirement in the U.S. Privacy Act of 1974.

[107] *Compare, e.g.,* 1995 EU Directive, Recitation No. 16 (national security), 17 (written and artistic expressions), and 36 (political opinions), and 1978 Foreign Intelligence Surveillance Act (national security exceptions and singling out of otherwise protected First Amendment activity). *See also* EU 2006 Data Retention Directive (creating exceptions for criminal law).

[108] *Compare* 1995 EU Directive, Recitation No. 28 and 1978 Foreign Intelligence Surveillance Act.

[109] *Compare* 1995 EU Directive, Recitation No. 30 and U.S. laws, *supra* note 5.

facilitate this structure, both regions also require that notice be provided to targets and that individuals have the right to access information that is held about them.[110] Individuals, in both systems, have the right to object to particular information, and in both systems, the data holder has a duty to ensure that the information is accurate and kept up to date.[111]

Keeping in mind the consistencies between the two systems, and the benefits to be gained for U.S. industry from emphasizing harmony, there are two areas where the two regions depart could be addressed through legislative reform: namely, recognition of residual rights in third party data, and the creation of a comprehensive, privacy-protective regime, as opposed to the piecemeal approach that currently marks U.S. law.

1. Residual Rights in Third Party Data

One central question that divides the United States from numerous other countries and regions—including the European Union—centers on who owns an individual's data. In the United States, since *Smith v. Maryland* (addressing pen registers and trap and trace devices), and *U.S. v. Miller* (focusing on financial records), all three branches have treated information held by third parties as lacking an individual right to privacy.[112]

In contrast, the European Union considers that the individual who has provided data to a third party to still have a privacy interest in the information.[113] The recent European Court decision, recognizing the right to anonymity, necessarily presupposes a continued interest in data, even once it is obtained by a third party.

The difference between the approaches is central to understanding how new technologies, such as social network analysis, cloud computing, and data mining, have deepened the privacy interests implicated in third party handling of data. New technologies allow information to be generated about which even those to whom the data relates are unaware. To say that individuals do not have a reasonable expectation of privacy in this information rather flies in the face of common sense.

The Supreme Court appears to be coming to this conclusion as well. In *United States v. Jones*, the Court considered a case involving 28-day surveillance involving the placement of a GPS chip on a vehicle.[114] Although ultimately decided on grounds of trespass, a shadow majority expressed strong concern about the implications of long-term surveillance. Justice Alito, joined by Justice Ginsburg, Justice Breyer, and Justice Kagan, suggested that in most criminal investigations, long-term monitoring "impinges on expectations of privacy."[115] The nature of new technologies mattered:

> Recent years have seen the emergence of many new devices that permit the monitoring of a person's movements. In some locales, closed-circuit television video monitoring is becoming ubiquitous. On toll roads, automatic toll collection systems create a precise record of the movements of motorists who choose to make use of their convenience. Many motorists purchase cars

[110] *Compare, e.g.,* 1995 EU Directive, Recitation No. 38 (notice) and 41 (right of access), and U.S. laws, *supra* note 5.
[111] *Compare, e.g.,* 1995 EU Directive, Art. 14 (right to object) and Art. 6 (accurate data); and U.S. laws, *supra* note 5.
[112] Smith v. Maryland, 442 U.S. 735 (1979); United States v. Miller, 425 U.S. 435 (1976).
[113] *See, e.g.,* 1995 EU Directive, Recitation No. 47.
[114] United States v. Jones, 132 S.Ct. 945 (2012).
[115] *Id.* at 964 (Alito, J., concurring).

> that are equipped with devices that permit a central station to ascertain the car's location at any time so that roadside assistance may be provided if needed and the car may be found if it is stolen.[116]

Justice Sotomayor went one step further, calling into question the entire basis for third party doctrine. Specifically, in light of the level of intrusiveness represented by modern technology, "it may be necessary to reconsider the premise that an individual has no reasonable expectation of privacy in information voluntarily disclosed to third parties."[117] Sotomayor pointed out:

> This approach is ill suited to the digital age, in which people reveal a great deal of information about themselves to third parties in the course of carrying out mundane tasks. People disclose the phone numbers that they dial or text to the cellular providers; the URLs that they visit and the e-mail addresses with which they correspond to their Internet service providers; and the books, groceries, and medications they purchase to online retailers.[118]

She continued, "I would not assume that all information voluntarily disclosed to some member of the public for a limited purpose is, for that reason alone, disentitled to Fourth Amendment protection."[119]

Congress has an opportunity to take the lead by recognizing the right to privacy still held by data holders when information is collected by third parties. It can then craft statutes accordingly, ensuring that U.S. companies offer greater protections for consumers, in the process allowing industry to offset the claims of its overseas competitors.

2. Legal Framework

Thus far, U.S. high technology companies have been subject to a very different statutory and regulatory structure than that which prevails in the European Union. In the United States, privacy rights have largely been protected via a series of vertical statutes dealing with specific areas, such as children using the Internet, driver-related information, and medical data.

In the EU, in contrast, privacy has been protected by a more omnibus-type approach, which horizontally reaches across a number of areas. This approach is reflected in the 1995 Directive as well as the national legislation implementing the directive on a country-by-country basis.[120]

The vertical statutory scheme has been successful in addressing particular, discreet areas where privacy interests reside. However, outside of these narrow exceptions, in the interests of encouraging innovation, the high technology sector has been left largely unregulated by federal statute. The assumption has been that market forces would adjust to protect privacy interests.

---

116. *Id.* at 963.
117. *Id.* at 957 (Sotomayor, J., concurring).
118. *Id.*
119. *Id.*
[120] *See, e.g.*, U.K. Data Protection Act of 1998, Germany's Federal Data Protection Act of 2001, France's Data Protection Act of 1978 (revised in 2004), Finland's Act on the Amendment of the Personal Data Act (986) 2000; Denmark's Act on Processing of Personal Data, Act No. 429, May 2000; Greece's Law No. 2472 on the Protection of Individuals with Regard to the Processing of Personal Data, April 1997.

The advantage of this approach has been to give high tech companies a significant amount of flexibility, allowing them to independently gauge the appropriate level of privacy protections to give to consumers.

The drawback has been that privacy itself has become commoditized, with companies actually making money off of selling consumers' privacy interests.

Consider Google and its email service, Gmail, for instance. The company reads and analyzes all of its customers' emails, it watches what people read, it looks at web sites people visit, and it records what people purchase. The company then sells access to customers' private lives to companies who want to advertise. Thus, the mother who sends an email to her son raising concern about depression may receive an ad within hours for psychiatric services, even as a pregnant woman merely looking at cribs, may within days receive mail through the U.S. post, advertising sales at Babies R'Us.

In September 2013 Google lost an effort in the 9th Circuit Court of Appeals for judicial review of a lower court's refusal to dismiss multiple class action lawsuits accusing Google of violating the Wiretap Act. U.S. District Judge Lucy Koh determined that the case is too far along to suffer delays. Koh's interpretation of the Electronic communications Privacy Act limits the "ordinary course of business" exception—not least because Google's practice violates its own policies.[121] The lawsuits, filed in California, Florida, Illinois, Maryland, and Pennsylvania, at great expense, are proceeding.

Capitalizing on private data represents a significant breach of the right to privacy. Instead of protecting privacy, the market has exploited it for monetary gain. In the United States and overseas, individuals are concerned about the lack of protections afforded. Congressional legislation could fix this problem by bringing high technology within the broader statutory framework and thus closing a gap in the existing law.

3. Safe Harbor Considerations

In the wake of the Snowden documents, the EU Commission issued a report recommending the retention of Safe Harbor, but recommending significant changes, including required disclosure of cloud computing and other service provider contracts used by Safe Harbor members.

The Safe Harbor provisions, developed 1999-2000 by the U.S. Commerce Department, the Article 31 Committee on Data Privacy, and the European Union, created a narrow bridge between the United States and EU. At the time, the European Parliament, which did not bind the European Commission, *rejected* the Safe Harbor provisions by a vote of 279 to 259, with twenty-two abstentions. Chief amongst European concerns was the failure of the agreement to provide adequate protections.

In light of the massive data breaches we have had over the past five years in the United States, the practices of a largely unregulated high technology industry, and the ubiquitous nature of NSA surveillance, Europeans are even less supportive of the Safe Harbor provisions. They amount to a self-regulated scheme in which the Federal Trade Commission merely looks at whether a company, which has voluntarily opted-in to the program, fails to do what it has stated it will do, within the bounds of its own privacy policy. Stronger measures are necessary to restore European confidence in U.S. high technology companies.

---

[121] In Re: Google Inc. Gmail Litigation, Case No. 5:13-md-02430, N.D.C.A.

C. Establishing Economic Security as National Security

Economic strength as national security, as was previously discussed, is not a new concept. The Founding itself was premised, in part, on the importance of economic security as being vital to U.S. national interests. In 1787 the Articles of Confederation were written out of existence on economic security grounds, as the country sought to reassure the international community that it was a viable trading partner. Since that time, the United States has at times had to remind itself of the importance of the economy to U.S. national interests. We are once again at such a time.

High technology is a vital part of the U.S. economy. It is both a symbolic and actual manifestation of the country's commitment to innovation in every sphere of life. It plays to the United States' strengths as a nation. It has the potential to change regimes, to alter political relationships, and to shape the daily lives of people around the globe. And it deserves special attention. The danger is that U.S. industry will become less competitive and that the U.S. will thus lose its dominance in the Internet economic sphere.

To some extent, we do, structurally, pay some attention to the importance of the economy. But many consequential decisions are thus not aired in full light of the possible implications for U.S. national security.[122] One way Congress could rectify this would be to take a look at how to integrate economic concerns, as a statutory matter, into the national security infrastructure.

V. CONCLUDING REMARKS

To redress the negative effects that have followed from public awareness of the NSA programs conducted under Section 215 of the USA PATRIOT Act and Section 702 of the FISA Amendments Act, the most important step that Congress could take would be to reign in the surveillance authorities themselves, in the process providing greater transparency and oversight. An alteration in U.S. privacy law would also help to reassure U.S. customers and individuals located outside domestic bounds that consumer privacy is protected, thus allowing industry accurately to assert that the circumstances have changed. Consideration of how to integrate economic concerns into the national security infrastructure would further help to emphasize the importance of taking account of the impact of new initiatives on the United States.

[122] *Id.*

Mr. TERRY. Thank you, Professor.
Mr. Heather, you are now recognized for 5 minutes.

STATEMENT OF SEAN S. HEATHER

Mr. HEATHER. Thank you, Mr. Chairman and Ranking Member, members of the subcommittee, for the opportunity to be here today.

Members of the U.S. Chamber, large and small alike, across all sectors of the economy rely on cross-border data flows to run their businesses as well as create better products and services. Let me share with you some examples of where cross-border data flows are necessary as part of today's economy.

From anywhere in the world, medical diagnostic equipment can now be serviced and even repaired remotely, saving valuable downtime. Financial transactions take place globally in the form of credit card services or the purchase or sale of stocks and bonds. Every package that ships has data associated with it, and as that package physically moves across borders so does the data electronically. Insurance companies store policy information in multiple server locations to be sure they can access it in case of disasters. And perhaps most obviously, any company with employees in multiple countries needs to have an IT network that moves company emails.

For all of these reasons and thousands more, we must understand that cross-border data flows affect all businesses, not just ICT companies. Despite the paramount importance of and benefits derived from having the ability to transfer data across borders, some foreign governments continue to push for restrictions on cross-border data flows. Within the last year, we have seen more than a dozen countries consider such measures.

Efforts to restrict cross-border data flows have been fueled by revelations regarding U.S. Government surveillance. This issue, while important, ultimately conflates concerns about Government access and use of data with commercial access and use of data. Attempts to limit the movement of commercial data ignore the fact that a completely separate legal regime often governs law enforcement activities.

In reality, foreign government efforts to require forced localization of servers or to put in place local content requirements are at their core often attempts to bolster homegrown ICT industries.

The Chamber, as a part of an educational awareness campaign in Indonesia earlier this year, assembled a panel of Indonesia ICT startups. Their message to their government underscored their need for cross-border data flows in order for them to be successful. Their voice has sent a powerful message that data localization efforts effectively walled them off from the rest of the world.

Still, some foreign governments believe that requiring data centers will be a boon to job creation. The truth is data centers cost hundreds of millions of dollars but require fewer than 150 employees to operate. Foreign governments often fail to realize that jobs are created by businesses that rely on cross-border data flows, exhibiting a fundamental failure to understand how the digital economy operates and running a risk of cutting the world out of the World Wide Web.

Cross-border data flow restrictions can also arise through the complexity of complying with privacy frameworks across multiple

jurisdictions. All companies must abide by privacy rules in the countries in which they operate. Many times privacy regulations from country to country are nuanced and rooted in important cultural and societal differences.

However, conflicting privacy rules between jurisdictions can present significant problems to moving data. Thus, it is imperative that governments work together to develop solutions to ensure that privacy regimes facilitate trade in goods and services that increasingly rely on data flows while protecting privacy.

This is especially important as consumers too are mobile and their expectations are that they can access information when traveling, while at the same time they have assurances that their data, regardless of where it is transferred, stored, or accessed, is protected. The Chamber believes privacy objectives and seamless movement of data can both be achieved.

Trade agreements can help. For example, the U.S.-Panama and U.S.-Korea Trade Agreement both recognize the importance of seamless flow of information. The Chamber's members support ambitious cross-border data flows obligations in the TPP, TTIP, and TISA. Ideally, these agreements should address data transfers by including three key elements: one, a commitment to allow cross-border data transfers; two, a prohibition on data localization and local content requirements; and, three, a nonexhaustive list of data transfer mechanisms.

In closing, the key takeaways from my remarks are, first, cross-border data flows are critical to all sectors of the economy, not just ICT companies; two, concerns over Government access and use of data will not be addressed through laws targeting commercial data; three, ICT industries are best fostered where data flows seamlessly; four, privacy concerns by Government must not mask protectionism aims; five, legitimate privacy objectives can be supported through cross-border cooperation between regulators; and, finally, going forward, trade agreements must support cross-border data flows, push back against forced localization and local content requirements, endorse the seamless flow of data, and encourage interoperability among privacy regimes.

It is well understood that the free flow of capital across borders is important to the global economy. Without it, markets seize up and economic growth stagnates.

Today I would submit, in this increasingly digital age, the same can be said about the importance of data flows across borders. Like capital flows, our economy and the world economy are relying on cross-border data flows for businesses to operate and for economic growth.

The Chamber appreciates the opportunity to be here before the committee. Today's hearing importantly raises the profile of this issue at a critical time. And we look forward to working with this committee to preserving the movement of data seamlessly across borders. Thank you.

[The prepared statement of Mr. Heather follows:]

Statement of the U.S. Chamber of Commerce

ON: Cross-Border Data Flows

TO: U.S. House of Representatives Committee on Energy and Commerce
Subcommittee on Commerce, Manufacturing, and Trade

DATE: September 17, 2014

The Chamber's mission is to advance human progress through an economic, political and social system based on individual freedom, incentive, initiative, opportunity and responsibility.

The U.S. Chamber of Commerce is the world's largest business federation representing the interests of more than three million businesses of all sizes, sectors, and regions, as well as state and local chambers and industry associations.

More than 96% of Chamber member companies have fewer than 100 employees, and many of the nation's largest companies are also active members. We are therefore cognizant not only of the challenges facing smaller businesses, but also those facing the business community at large.

Besides representing a cross-section of the American business community with respect to the number of employees, major classifications of American business—e.g., manufacturing, retailing, services, construction, wholesalers, and finance—are represented. The Chamber has membership in all 50 states.

The Chamber's international reach is substantial as well. We believe that global interdependence provides opportunities, not threats. In addition to the American Chambers of Commerce abroad, an increasing number of our members engage in the export and import of both goods and services and have ongoing investment activities. The Chamber favors strengthened international competitiveness and opposes artificial U.S. and foreign barriers to international business.

Positions on issues are developed by Chamber members serving on committees, subcommittees, councils, and task forces. Nearly 1,900 businesspeople participate in this process.

The U.S. Chamber of Commerce is pleased to take this opportunity to address the importance of cross-border data flows to the U.S. business community. The Chamber is the world's largest business federation, representing the interests of more than three million businesses of all sizes, sectors, and regions, as well as state and local chambers and industry associations, and is dedicated to promoting, protecting, and defending America's free enterprise system.

The movement of information across national borders drives today's global economy. Cross-border data flows allow businesses and consumers access to the best available technology and services, wherever those resources may be located around the world. The seamless flow of data across borders benefits all industry sectors, from manufacturing to financial services, education, health care and beyond. The seamless transfer of information is as critically important as it is inexorably linked to the growth and success of the global economy.

To function in the international marketplace, businesses need continuous, reliable access to data, wherever they are located. Routine business activities, such as providing goods and services to customers, managing a global workforce, and maintaining supply chains, require the transfer of data among corporate locations and to service providers, customers, and others situated around the world. In addition, as the Internet has facilitated the growth and success of micro-multinationals, as small businesses now have access to billions of potential customers beyond their borders and are able to compete based on the quality of their offerings, unconstrained by geographic limitations.

The global value of e-commerce is estimated at $8 trillion per year. And this amount is not limited just to large multinational technology companies: 75 percent of the value-added created by the Internet is generated by companies in traditional industries, such as manufacturing, and small- and medium-sized enterprises that rely heavily on Internet services have 22 percent greater revenue growth than companies that do not.

A survey released this week by the International Trade Commission found that digital trade increased U.S. GDP by $517.1-$710.7 billion (3.4-4.8 percent) as U.S. firms sold $935.2 billion in products and services online in 2012. With 95 percent of the world's consumers located outside of the U.S. borders and the world population increasingly connecting online, this number is only poised to grow. Consequently, we must work to ensure that the United States remains a worldwide leader in this economic revolution and that American companies have access to the world's growing middle class.

Despite the myriad benefits of transferring data between countries, some governments continue to push for restrictions on cross-border data flows. This limits the ability of companies to process, store, and access information on a global basis, and impedes end users from being able to choose the best available technologies and access information regardless of location.

Recent restrictions proposed in response to allegations regarding foreign government surveillance inappropriately conflate concerns about access to data for national security and law enforcement purposes with commercial use of, and access to, data. Other restrictions are rooted in government efforts to bolster domestic industry and support national companies. Ultimately, however, instead of creating jobs, these rules reduce efficiency, increase costs to local businesses, and block access to customers abroad, as they simultaneously prevent local

consumers from buying the best products and services. Restrictions on cross-border data flows only serve to isolate domestic economies from the economic growth potential associated with the digital economy.

Uses of Cross-Border Data Flows

Policymakers and citizens often fail to appreciate the many benefits of cross-border data flows in their day-to-day lives. Maintaining the ability to transfer data is not just essential to business operations and revenue growth, but it also facilitates socially beneficial global initiatives and help improve the health and well-being of people around the world. Chamber members, across all sectors, rely on cross-border data flows for a variety of function, and it is important to highlight that most companies are not using or selling the data itself as a cash generative business, but are using it to create better products and services.

Medical Data

A number of multinational medical device manufacturers routinely transfer data across jurisdictional boundaries for maintenance and repair purposes.[1] For instance, one device manufacturer lamented the difficulties engineers face when attempting to carry out critical functions, such as providing real-time service on large medical equipment to facilitate effective patient care. Sophisticated equipment of this nature often cannot be readily transported to repair facilities, and in some cases the device requiring service is the only machine of its type in a particular geographic area.

If an engineer who is specially trained to service a highly complex machine is not permitted to access the device remotely to conduct repairs (because she may incidentally access the data of patients who benefitted from the machine that morning), then patients who need the machine that afternoon may be turned away. In this example, cross-border data transfer restrictions literally could have life or death consequences for patients. Some of the data that is transported are used for purposes well beyond commercial purposes, including public health and safety concerns.

Stopping Fraud

Cross-border data flows are used to identify fraudsters who, after racking up huge debts in one country, are able to start fresh with a clean slate by moving to another jurisdiction. Blocking credit histories from following individuals across borders also affects law-abiding expatriates who are unable to open accounts or obtain loans because they have no way to prove they have a strong credit history in their country of origin.

---

[1] In addition to medical devices, other types of machinery may be repaired in a virtual environment, thus sparing consumers time and effort. For example, a recent report highlighted the fact that Tesla Motors is now able to make safety changes to plug-in electric vehicles using "over-the-air software updates," calling into question the use of the term "recall" when discussing this type of maintenance. *See* Angela Greiling Keane, *Tesla's Musk Has Point About 'Recall,' Ex-Regulator Says*, BLOOMBERG NEWS, Jan. 21, 2014, http://www.bloomberg.com/news/2014-01-21/tesla-s-musk-has-point-about-recall-ex-regulator-says.html (last visited Apr. 22, 2014).

Creating Efficiencies for Manufacturing and Energy Development

One of our members operating in the energy sector uses cross-border data flows to help oil and gas manufacturers function at top capacity while promoting safety and ensuring continuity of service. To achieve this, the company remotely collects operational data from equipment in use in locations scattered across the globe, then employ diagnostic and prognostic analyses of the data to alert customers of necessary maintenance and potential risks. Hampering companies' ability to monitor the data transmitted by such equipment from around the world both decreases efficiency and increases the likelihood of a preventable accident that could damage infrastructure and even result in loss of life.

Responding to Remote Crises

The insurance and reinsurance industry offers another strong argument in favor of allowing the rapid and nimble movement of data across borders. In the event of a major natural disaster, immediate access to clients' insurance contracts and records is essential to deploying needed resources to policyholders and helping begin the rebuilding process for affected individuals. When cross-border data transfer restrictions impede the movement of these data, or restrict the storage of such data outside the country of origin, the results can be disastrous. For example, if a particular country requires an insurer to maintain all its data pertaining to citizens of that country within the country's borders, the insurer may have no way to access the data it needs to help affected residents recover from a tsunami, earthquake, or other major disaster. If the data center is under 10 feet of water, it is impossible assess who has coverage or how to start processing valid claims. The ability to maintain backup copies of insurance coverage data in multiple remote locations helps the company ensure continuity of service even in the face of massive power outages and physical destruction of servers or other company property that typically would be used to validate coverage and provide assistance.

Managing a Global Workforce

Regardless of industry sector, all companies large and small have one thing in common: employees. Perhaps no commercial data transfer need is as acute, or as universal, as the need for companies to be able to access data about their workforce around the world. Having a complete and accurate picture of the company's personnel, wherever in the world they may sit, is essential to deploying and managing intellectual capital effectively. A centralized corporate directory, the existence of which could be threatened by stringent data transfer restrictions, also is key for obvious logistical purposes. Furthermore, innovation is driven by cross-cultural project teams collaborating in virtual environments, working together to solve problems and develop products from locations around the world. And IT technicians staggered across time zones help ensure that assistance is always available for employees working unconventional hours or logging in from remote locations. Modern businesses simply cannot thrive, or even function effectively, without the ability to manage their talent on a global basis.

Tracking Pandemics, Saving Lives

The Internet has proven to be an invaluable resource for global health organizations, enabling them to make massive leaps forward in monitoring the outbreak and spread of infectious diseases around the world. But this type of tracking is possible only through the rapid

collection and dissemination of real-time medical data concerning patients in multiple countries. Owing in part to increasing globalization and modern transportation, what may appear as an isolated cluster of illness in one region of one country easily could explode into a national epidemic or a global pandemic in a matter of weeks or even days.

Unless epidemiologists and other medical professionals are able to communicate freely about emerging health crises with their colleagues located elsewhere, there is little the medical community as a whole can do to slow or stop the spread of disease outbreaks.

Restrictions on Cross-Border Data Transfers

Localization requirements also may have the effect of decreasing data security. Forcing companies to maintain local data centers frequently results in the establishment of minimally-resourced facilities that are more likely to permit network intrusions and data compromises. In the end, compliance costs are passed on to consumers when prices for goods and services are increased to fund local outposts rather than having centralized service centers that maximize efficiency. In addition, data transfer restrictions often have a disproportionate effect on smaller businesses, in some cases potentially thwarting growth opportunities altogether and preventing today's startups from becoming tomorrow's multinationals. For these businesses, data transfer restrictions have the effect of cutting the "world" out of the "World Wide Web."

Despite the multitude of benefits associated with allowing data to flow seamlessly across borders, governments around the world continue to step up efforts to impose restrictions on cross-border data transfers. Although in some cases the restrictions are meant to promote privacy, too often the motives are protectionist or reflect the conflation of commercial issues with national security concerns. These misguided policy choices take us down a path that stifles job growth and leads to economic stagnation.

Unfortunately, regardless of intent, many of the regulations affecting the commercial use of data impose unduly restrictive constraints on international data flows, doing more harm than good to the affected economies. Initiatives aimed at improving data transfer regulations should refrain from focusing on a single set of rigid, one-size-fits-all rules. Instead, such initiatives should focus on developing flexible, privacy-protective regulations that can coexist with, and adapt to, technological advances.

Data transfer restrictions generally fall into two categories: data localization requirements and privacy regulations. Data localization rules, which usually are binary in nature, impose an outright ban on transferring data out of the country, or a requirement to build or use local infrastructure and servers. These regulations often are based on misperceptions that are easily refuted. Accordingly, it is more effective to demonstrate the flawed reasoning behind the laws and persuade policymakers to repeal them altogether, rather than attempt to find common ground on the localization issue.

Conversely, privacy regulations are nuanced and rooted in important cultural and societal concerns. Such rules generally seek to protect legitimate interests and fundamental rights. Thus, it is imperative that governments work together to understand the underlying interests when developing solutions to ensure that local privacy regimes do not unnecessarily restrict trade. Furthermore, procedures to protect privacy and secure data are vital to modern business

operations. Given the concerns of consumers and governments alike, companies strive to develop trustworthy products that meet privacy expectations. Increasingly, those expectations include ensuring that privacy protections travel with the data, regardless of where they are transferred, stored, or accessed.

In the past year, high-profile revelations regarding government surveillance activities resulted in a number of proposals regarding data localization and transfer restrictions. Although some of the adverse reactions are understandable, thus far most of the efforts to alleviate concerns regarding surveillance have failed to address the real issue. A useful step in the right direction would be for members of Congress to more vocally distinguish between issues of law enforcement and national security collection and use of data with that of the private sector.

The means by which governments access foreign personal data should have no bearing on the laws that regulate corporate data transfers or the mechanisms companies employ for cross-border transfers. The political rhetoric connecting government surveillance to commercial data transfers ignores the fact that a completely separate legal regime often controls law enforcement access to data. Efforts to reform government surveillance must directly address government actions – these concerns cannot be resolved by creating new restrictions on businesses.

Separating Fact from Fiction: Forced Data Localization

During the last few years, there have been a number of data localization proposals around the world. Whether in response to national security surveillance concerns, a desire to protect domestic industry or some combination of the two,[2] these proposals are based on a number of false assumptions and ultimately fail to meet any of the stated goals.

Myth: Data localization will promote domestic industry.

Fact: Data localization requirements reduce competitiveness by walling off domestic businesses from the billions of potential customers outside of the home country's borders. This isolation reduces investment and access to capital – the ability to assess a potential borrower's creditworthiness or to spot potentially fraudulent activity often depends on the ability to move data across borders.

Myth: Requiring local data centers will create jobs.

Fact: Jobs are created by businesses that leverage a global network of data centers, using the best available technology to increase efficiency regardless of location. This enables domestic industries to focus on the quality of their products and services, better positioning them to compete in global markets. Data centers can cost hundreds of millions of dollars to build and operate, and even a cutting-edge data center requires fewer than 150 workers.

---

[2] *See, e.g.*, Press Release, Eur. Comm'n, What does the Commission mean by secure Cloud computing services in Europe? (MEMO/13/898) (Oct. 15, 2013), *available at* http://europa.eu/rapid/press-release_MEMO-13-898_en.htm (last visited Apr. 30, 2014) (proposing the creation of a virtual "Schengen Area" for data in response to surveillance revelations and supporting the development of European cloud computing solutions).

Myth: Data localization increases security.

Fact: Data security depends on a plethora of controls, not on the physical location of a server. Businesses often back up data outside the country in which it is collected to help ensure it remains secure in the event of a natural disaster, power outage or other such emergency that could take a data center offline. Businesses and consumers benefit when those who maintain data are able to use the best available security measures, regardless of the physical location of the data they seek to protect. Geographic neutrality with regard to data storage enables all companies, particularly small ones, to employ cost-effective information security solutions.

Myth: Data localization will lower costs for domestic business.

Fact: Requirements for local servers could hurt domestic industry by compelling local businesses to sacrifice efficiency and seek out more expensive, less reliable services. Localization requirements may limit the ability of firms to access logistics and supply chain infrastructure, conduct effective research, secure appropriate insurance, or readily participate in financial markets.

Opportunities for International Cooperation in Trade Agreements

The ability to transfer data across borders has become inextricably intertwined with the ability to trade freely. Current trade discussions, such as the U.S. – EU Transatlantic Trade and Investment Partnership (TTIP) and the Trade in Services Agreement (TISA), present opportunities to bridge differences among privacy regimes and developing regional data transfer mechanisms.

Data Transfer Provisions in Trade Agreements

Addressing cross-border data transfers through trade agreements is not a novel approach. A number of trade agreements have even acknowledged the significance of cross-border data transfers to the global economy as a fundamental tenet of the agreement. For example, Article 14.5 of the U.S.-Panama Trade Promotion Agreement highlights the importance of helping small- and medium-sized enterprises "overcome obstacles" that impede their participation in electronic commerce and maintaining "cross-border data flows of information as an essential element in fostering a vibrant environment for electronic commerce."[3]

Similarly, Article 15.8 of the United States-Korea Free Trade Agreement (KORUS) recognizes "the importance of the free flow of information in facilitating trade" and pushes the parties to the agreement to "refrain from imposing or maintaining unnecessary barriers to electronic information flows across borders."[4]

---

[3] Trade Promotion Agreement, U.S.-Pan., art. 14.5, June 28, 2007, *available at* http://www.ustr.gov/trade-agreements/free-trade-agreements/panama-tpa/final-text (last visited Apr. 22, 2014).

[4] Free Trade Agreement, U.S.-S. Kor., art. 15.8, June 30, 2007, 46 I.L.M. 642. Both the KORUS and the EU – Korea Trade Agreement (KOREU) include provisions specific to financial services, with KOREU stating "each Party shall permit a financial service supplier of the other Party established in its territory to transfer information in electronic or other form, into and out of its territory, for data processing where such processing is required in the ordinary course of business of such financial service supplier." Free Trade Agreement, Eur. Union-S. Kor., art. 7.43, Aug. 20, 2010, 2010/0075 (NLE).

In addition, the Chamber's members support an ambitious Trans-Pacific Partnership Agreement (TPP) that preserves the ability to transfer data across borders and look forward to a final TPP is likely to include provisions aimed at preventing member countries from adopting national laws that would restrict cross-border transfers of personal data. Despite these positive steps, more needs to be done to embed strong, binding commitments in future agreements.

The Transatlantic Trade and Investment Partnership

The TTIP represents one of the best opportunities to institute cutting-edge data transfer protections, notwithstanding misplaced concern related to U.S. government surveillance issues. Ideally, the TTIP should address data transfers by including three key features: (1) a commitment to allowing cross-border data transfers; (2) a prohibition on data localization requirements; and (3) a non-exhaustive list of data transfer mechanisms. In conjunction with the third issue, the agreement should also ensure ongoing cooperation between the United States and EU with respect to developing new data transfer mechanisms. The TTIP also must meaningfully limit the transfer prohibitions allowed under the General Agreement in Services (GATS) Article XIV.[5] If the United States and the EU are able to implement strong and ambitious provisions in the TTIP, that agreement may serve as a template and baseline for the TISA negotiations that will affect nearly 70 percent of the global economy.[6]

Conclusion and Recommendations

Cross-border data transfers are indispensable to the growth of the digitized global economy. Cross-border data transfers are critical for all modern business. The global economy simply cannot afford to revert to digital isolationism. The question is whether governments will implement legal regimes to promote a beneficial expansion of the data economy, or if the cumbersome systems currently in place will continue in force, hindering innovation and slowing progress. The path forward must include cooperation between regulators and businesses working together to determine how best to address important concerns about privacy and data security without crippling economic growth.

Regardless of the specific geographic or political context, the following key concepts are critical to ensuring agile cross-border data transfer regimes that will facilitate the global data flows of the future:

- Recognition that there are many different approaches to regulating cross-border data transfers, and that differing mechanisms can ensure a similar desired level of data protection.
- Movement away from rigid one-size-fits-all regulations toward more outcome-focused regimes.
- A clear delineation between the issue of government access to data and the distinct issue

[5] General Agreement on Trade in Services art. XIV, Apr. 15, 1994, 1869 U.N.T.S. 183, *available at* http://www.wto.org/english/docs_e/legal_e/26-gats_01_e.htm#articleXIV (last visited Apr. 30, 2014).

[6] OFFICE OF THE U.S. TRADE REPRESENTATIVE, NOTICE NO. 2013-21836, PARTICIPANTS IN TRADE IN SERVICES AGREEMENT (2013), *available at* http://www.regulations.gov/#!documentDetail;D=USTR_FRDOC_0001-0270 (last visited Apr. 22, 2014).

of cross-border data transfers in a commercial context.

- Assurance that the frameworks we develop today are fit for tomorrow.
- Implementing strong, binding trade agreement commitments that prohibit data localization requirements, support unimpeded data flows, and encourage interoperability among privacy regimes.

Technological advances and an increasingly globalized economy have brought us to a policy crossroads: one path leads to a "splinternet" of economic isolation, characterized by misguided attempts to safeguard data by building protectionist walls. Since the dawn of the global trading system, this isolationist approach has repeatedly caused economic stagnation. The other path is one of shared global economic growth fueled by an increasingly interconnected digital economy. Ideally, this would be supported by regulatory frameworks that encourage competition by opening borders for businesses of all sizes, driving innovation, creating jobs and lowering prices.

The Chamber encourages Congress to seize the opportunities presented at this critical juncture and push towards preserving the ability to transfer data across border and in turn continue the flow of benefits.

Mr. TERRY. Thank you, Mr. Heather.

And well done, everyone. Appreciate the input. Now it is our turn to ask questions to kind of dive deeper into your statements.

But just my first question is a shallow question, but one that helps us really define the significance of cross-border data. And so to Ms. Dempsey, Bieron, and Mr. Heather, can you, in your best estimate, tell us just either by dollar amount or the percentage of your members or clients engage in cross-border data transfers? Ms. Dempsey? Hundred percent? Fifty percent? Ten percent?

Ms. DEMPSEY. Thank you, Mr. Chairman. That is a tough one to answer quantitatively for NAM. I think information technologies are clearly a driver of global trade. And the growth in global trade that we have seen, particularly among small businesses, has been driven in significant part by that. We obviously have over $200 billion last year in actual computer and electronic equipment, but the gains are much, much more than that. But beyond that quantification——

Mr. TERRY. OK.

Mr. BIERON. In the United States, the eBay commercial sellers—so these would be when we have done our research globally, we sort of pick $10,000 in sales a year simply because we had to pick a number and that seemed like a nice round number—so at that level in the United States, 97 percent of them are exporting. And so they are interacting with customers globally. And that number, in the upper 90s, tends to be with our commercial sellers almost everywhere in the world. So it is nearly everybody.

Mr. TERRY. So out of that group, 97 percent. But how big is that group?

Mr. BIERON. Hundreds of thousands in the United States and, you know, about 2 times that globally.

Mr. TERRY. Awesome.

Mr. Heather.

Mr. HEATHER. I, like the NAM, have a hard time quantifying what the number would be in the U.S. Chamber's membership. But I think, from talking with our members, what you see is the frequency by which they are increasingly relying on cross-border data flows. So you may have a small business that 5 years ago only once may have been looking online to source a product that they needed outside of the United States, and today they are doing that a dozen times in a year.

And so what I can speak to more is the frequency in which companies are increasingly relying on cross-border data flows, but some absolute number to give you across the membership would be difficult.

Mr. TERRY. All right.

Professor Donohue.

Ms. DONOHUE. Yes. Just to add to that, outside of e-commerce, for the IP industry alone about 40 million American jobs are tied directly to IP-intensive industries, which stimulate about 60 percent of our exports, our merchandise exports. So it is enormous numbers.

Mr. TERRY. They are enormous numbers, and that is why we want to set the table about how important this is.

The next part is we have all talked about how this has to be discussed and negotiated in our trade agreements. Do you think it would help Congress to weigh in with some level of resolution, instructing or suggesting to USTR and the Department of Commerce? Would that be helpful? And we will start from right to left, just to be different.

Mr. Heather.

Mr. HEATHER. I think absolutely. If you look at language that has been drafted in, for example, the trade promotion authority legislation that has been out there for examination, there is very positive language in that proposed legislation on this issue. I think it would be important for this committee to echo that, not only in order to give encouragement to the U.S. Chamber of Commerce, who are working these issues hard, but to send a signal to those trading partners that there is an expectation that USTR brings that home when they bring home an agreement for the Congress to consider.

Mr. TERRY. Professor Donohue.

Ms. DONOHUE. So I would say it is not just important, but essential that this committee actually weigh in on that. And it is essential that they both weigh in on the importance of data flows and data transfers and also doing something to give our industry the ability to say things have changed, to increase consumer confidence.

So really going after the source of the problem that is really accelerated this movement toward data localization, to say, no, we have now curved these surveillance authorities, they are more transparent, we have more oversight. So you take away the reason people might give for otherwise doing this. And this committee can play a unique role in both ways.

Mr. TERRY. Mr. Bieron.

Mr. BIERON. In a word "yes." And to expound on that, I think that trade negotiations and the global trade sort of infrastructure moves very slowly. We all know that trade agreements tend to be built on the previous trade agreement, which is built on the previous trade agreement. They all take, let's say, a decade to negotiate.

When you are dealing with the changes that are wrought by the Internet where the global economy is changing so rapidly, they very much need a very forceful direction to rapidly change how the Internet is accounted for in our negotiating objectives, because if we move our trade policy at the normal speed that it moves, we will, like, miss most of what is happening in the Internet.

Mr. TERRY. That is a good point.

Ms. Dempsey. And I am out of time, so make it quick.

Ms. DEMPSEY. I agree. And I will just add, I concur with all that my colleagues have said. It is so important for the United States to speak with one voice on this issue. It is moving fast. We are seeing this proliferation of other countries trying to impose very protectionist policies under the guise of security or privacy concerns. It is important for you all to work together to move this issue forward.

Mr. TERRY. Thank you.

Gentlelady from Illinois is recognized.

Ms. SCHAKOWSKY. Thank you, Mr. Chairman.

Mr. Bieron, I have—did I say that right?

Mr. BIERON. Yes.

Ms. SCHAKOWSKY. OK. I have a number of questions for you. One of the reasons other countries are considering laws that restrict cross-border data flow is the fear that their personal and financial information is not being properly protected from criminal cyber attacks. Earlier this year, this subcommittee held a hearing on the Target and Neiman Marcus data breaches that occurred late last year. And since then, we have heard of a number of other large-scale data breaches, Michaels, Home Depot.

In May of this year, news broke that eBay's system had been breached and an unknown number of eBay's 145 million customers' personal information, including names, phone numbers, home address, emails, and encrypted passwords, were compromised. So I am asking you if you have any sense now, more than 3 months after the breach, of how many customers had their data exposed during the breach?

Mr. BIERON. I don't believe that we know exactly how many customers had their data accessed. The cyber attack that resulted in the essentially stealing of names—as you said, names, addresses, phone numbers—did prompt eBay to ask and require all of our users to change their passwords before they could reaccess the site.

So what it prompted, in our case, was the decision to, for safety's sake, require everybody to change their password, because user passwords, although accessed in an encrypted form, they were accessed, encrypted passwords were accessed. And we decided that the smartest and safest thing to do was to require a password reset, which we implemented.

Ms. SCHAKOWSKY. Did the breach compromise eBay's customers in countries other than the United States?

Mr. BIERON. It impacted our eBay customers globally.

Ms. SCHAKOWSKY. So I am sure you recall that eBay received some criticism at the time the breach was announced about its public response to the attack. There was an article in Wired which noted that the initial warning about the breach was a note on the eBay corporate Web site, not eBay.com. A statement was also posted to PayPal's Web site that warned in its title that eBay users should change their password, but the body of the post offered no information, other than the words, quote, "placeholder text," unquote.

And so in what ways, then, did you notify customers that they should change their password, other than that?

Mr. BIERON. Well, I mean——

Ms. SCHAKOWSKY. PayPal.

Mr. BIERON. Sure. When we discovered that there had been a breach of our system, the company rapidly worked to determine what the extent of that breach was, when it was determined, what the extent was. And we realized that the proper course of action would be to have everyone reset their password.

Ms. SCHAKOWSKY. You still don't have a number?

Mr. BIERON. No. We still don't have a number because data files we know were accessed that had names and addresses and passwords and phone numbers. And as I would note, the passwords

were encrypted. They were accessed, but even now the exact number of the data points in the files, we don't know exactly how many ended up being withdrawn. So we know that——

Ms. SCHAKOWSKY. Well, I am just asking a simple question: How many customers had their data exposed, not what happened or——

Mr. BIERON. And that is what I am saying, we do not know based on how the breach occurred exactly the number that was accessed.

Ms. SCHAKOWSKY. Don't think that is important, and how are you proceeding then?

Mr. BIERON. Well, how we proceeded was to require all of our customers to reset their passwords.

Ms. SCHAKOWSKY. So are you ever going to know?

Mr. BIERON. I am not sure if our technical people will ever know exactly the number. We do know that all of our users have had to reset their passwords because of that. And actually I believe that we have received quite a bit of praise for how rapidly we were able to put in place a system to have everybody have to reset their passwords and to notify all of our users.

Ms. SCHAKOWSKY. OK. Well, let me ask you. Different countries have different laws regarding breach notification. So how does eBay handle notification in the many different countries in which it operates, or did you have the same procedure, just change your password?

Mr. BIERON. We had the same procedures. We notified everybody. And then when they were coming to our site, they were stopped from proceeding and using the site until they changed their password.

Ms. SCHAKOWSKY. In addition to that, have you made any changes to your security and breach response procedures since May that would respond to any future attacks?

Mr. BIERON. Yes. I think that I would prefer, if we could, to respond in writing to give you a specific set of examples of things that we have done. But there is no question that the company looked very much at the kind of threats that are always coming at an Internet business like ours and did make some changes to address the way that this attack occurred.

Ms. SCHAKOWSKY. Thank you. I yield back.

Mr. TERRY. Gentleman from New Jersey, vice chairman of the subcommittee, is recognized for 5 minutes.

Mr. LANCE. Thank you very much. And I did change my password on eBay.

Ms. Dempsey, one of the chief concerns of the Energy and Commerce Committee and certainly this subcommittee is to promote the policies that reinvigorate the American manufacturing economy and we hope create jobs here at home. What do you think restrictions on data flows would have as a result, based on what we would like to do to reinvigorate the American economy?

Ms. DEMPSEY. Thank you, Congressman. And thank you for the work of this committee.

On manufacturing, obviously, it is NAM's mission to grow manufacturing in the United States. My position is to grow manufacturing through international trade policies and investment policies.

Restrictions on data flows, server localization barriers are going to drive a stake through the heart of the growth in manufactured exports that we have witnessed over the past decades. We have seen more than a doubling of U.S.-manufactured exports since 2002. We are at a record high, $1.38 trillion in manufactured exports, which helped fuel the biggest manufacturing output for the United States of over $2 trillion in 2013. That is great news.

The bad news? There is $11 trillion traded outside our borders in manufactured goods every year. The United States, while we have increased manufactured goods exports, we have lost market share. Our ability to compete overseas is increasingly tied to different policies. Eliminating barriers overseas, as I indicated, with new trade agreements.

These are some of the barriers that are becoming most pernicious and are continuing to grow. We can succeed when we have strong trade agreements, when we eliminate these barriers overseas. We see that with our trade agreement partners. So if we want to continue to grow exports and continue to have that to be a source of manufacturing growth, eliminating these types of barriers will go a long way.

Mr. LANCE. And we have lost market share because the pie has grown so much?

Ms. DEMPSEY. Yes. So other, new emerging countries. China, obviously. The United States used to be the largest manufactured goods exporter. We were overtaken by Germany and then by China. We are number two. And we are doing well, but we can do better. And we have a lot of other countries out there who are working hard.

But I will say that some of the countries that are really growing are those that are doing more to grow export opportunities, grow trade agreements. I am always disheartened to hear that companies are sometimes choosing Mexico as a venue to put new factories. Not because of NAFTA. It is because Mexico has a trade agreement with Brazil, and they have a lot more in Japan and a lot more trade agreements than we do that eliminate barriers.

So those are the types of things that impede us and putting the United States back on the track to lead and lead in the types of rules that we are going to have in the international economy.

Mr. LANCE. Thank you.

Is there anyone else on the panel who would like to comment?

Seeing none, Mr. Chairman, I will yield back the balance of my time.

Mr. TERRY. Thank you.

I recognize the gentleman from California. You are recognized for 5 minutes.

Mr. MCNERNEY. Thank you, Mr. Chairman. I am glad I came to the hearing today. It is a very interesting discussion, and I appreciate that.

I am going to start with you, Professor Donohue. Your testimony was pretty stark actually. I was on the Privacy Working Group, so I have heard some of this before, the impact of NSA activities and the disclosures about that on American businesses. And it is not very comforting.

You said that this subcommittee has a role to play in restricting NSA. Would you give us some suggestions or ideas.

Ms. DONOHUE. Sure. Sure. Thank you, Congressman McNerney. I appreciate it. It is nice to see you again.

I think there are three roles, really, that this committee could play. The first role is in supporting legislation passing through Congress right now dealing with the Foreign Intelligence Surveillance Act. Now, there are many bills underway. Some of them accomplish different things to different extents. But something needs to be done. Otherwise, our industry and our USTR are in a position where they can't really argue changed circumstances at all. And so I think it is very important that something be done.

The second thing that this committee can do is to take a look at the privacy laws and the ways in which consumer privacy is or is not actually protected. So the U.S. and the EU, a lot of ink has been spilled about how the two countries are so different in terms of their privacy laws. I disagree. And my written remarks go into some detail as to why I think we are actually not that far apart from Europe.

But two ways in which we differ significantly that are important are, first, in terms of third-party data and, second, in terms of having an omnibus statute as opposed to single statutes that drill down deeper, but in very narrow areas. In the second instance, Europe has broader statutes, directives that cross different areas. We have more narrow ones.

So one thing that this committee could do is look at a more overarching framework. The Privacy Act is 40 years old this year and is really a defunct piece of legislation. So that needs to be looked at.

The first part of this, though, the third-party data rights, the idea that you still have a right in information, even though a third party holds it or a company holds it. Our case law comes from the 1970s, from Smith v. Maryland. And we have seen recently that the Supreme Court is coming to the conclusion that the privacy implication and the privacy rights implicated by new technologies are significantly deeper than they were at a time when all we had were land lines. Now your cell phones tells where you are 24 hours a day, who you are with, what you are doing, what you read, what you believe, all of this information.

And so this committee could get out ahead of the Supreme Court in some ways and really recognize a consumer right to privacy in an omnibus statute and in this way bring the U.S. into line with the European Union on our own terms, but in a way that again helps our USTR and TTIP and other negotiations.

Mr. MCNERNEY. I mean, that sounds like something that could happen on a bipartisan basis as well.

Ms. DEMPSEY. Oh. Absolutely. Yes. Yes.

The third, and this has gotten almost no attention, but I have been really struck actually, and I say this as a scholar, just looking at how this has played out, the National Security Act does not include the Secretary of Treasury on the National Security Council. So PPD–1 does. That is up to the President.

And when international economic issues are on the agenda, then the President may invite the Secretary of Commerce, the USTR,

the Assistant to the President for Economic Policy, or the Chair of the Council of Economic Advisors to NSC meetings.

The problem is, if the issue isn't front-and-center international trade or international implications, that economic representation is not there, the consumer side of this, the commercial side of it, everywhere from the NSC down to a programmatic level. And so there are ways that the national security infrastructure fails to take account of the things that this committee cares about in a way that would help to prevent this kind of situation from arising in the future. And I think the committee could play a very strong role there by insisting that economic security, which from the founding has been central to U.S. national security, that economic security be taken into account as well.

Mr. MCNERNEY. Thank you.

Mr. Chairman, I was wondering if I could have another 5 minutes. Just joking.

Mr. TERRY. No. You can have 53 seconds.

Mr. MCNERNEY. Mr. Heather, I think on your closing statement you had five items that you mentioned. And the second one I think you mentioned was that data-flow problems cannot be addressed directly by dealing with commercial data. Did I misunderstand that?

Mr. HEATHER. The second point was that concerns about Government use of data and access of data are not going to be addressed with regard to laws about commercial data. In other words, concerns about NSA often conflate commercial use of data versus Government use of data. So the solutions to dealing with concerns about Government use are going to be different than solutions for use by commercial data.

Mr. MCNERNEY. Yes. Well, that is in line with what Dr. Donohue was saying, basically.

Mr. HEATHER. Correct.

Mr. MCNERNEY. All right. Mr. Chairman, I will yield back.

Mr. TERRY. Thank you. I appreciate that.

Now Mr. Bilirakis, gentleman from Florida, is recognized for 5 minutes.

Mr. BILIRAKIS. Thank you, Mr. Chairman.

And I thank the panel for their testimony today.

Mr. Bieron, you mentioned in your testimony that over 95 percent of small U.S.-based businesses using the eBay marketplace platform engage in exporting versus 4 percent of traditional businesses. Can you explain how you arrived at these figures? In particular, what is a traditional business in this context?

Mr. BIERON. Well, that was based on comparing data from the eBay marketplace with data that, I believe, was Census Bureau data that we had and a trade economist at the University of Geneva actually analyzed. So U.S. Government data on small business and their trading in the traditional economy compared to the percentages of exporting going on over our marketplace.

Mr. BILIRAKIS. OK. Thank you. Next question, again, for Mr. Bieron. Your testimony says that smaller businesses are reaching roughly 10 times as many markets per year than the traditional U.S. businesses. Please explain the difference in these markets and their importance to the overall business growth.

Mr. BIERON. That was simply data to explain sort of the difference between the kind of global marketing that a small Internet business can do. And again they are not businesses that, like, just exist on the Internet. These are small storefront businesses in many cases that also use the Internet. So they are selling locally, and they are also able to reach anyone who uses the services that they use. So if they are up on eBay, they are being seen by 140 million customers potentially around the world.

So the traditional business export model for small businesses tends to be—and this is why only about 4 percent do it—oftentimes they are small businesses that are either located near a border, so they have customers coming across the border regularly, or they have family connections, let's say, to a particular country, so they have export relationships through that. Or maybe they are a business that is part of another bigger business' supply chain. So maybe they are supplying a particular business in another country. This is why small businesses traditionally have oftentimes only exported to one or two countries a year.

In the Internet global business model, where you can be a really tiny business but now you are literally being seen by individual customers around the world and you are using your Internet, combined with services like eBay and PayPal, combined with then UPS, FedEx, the Postal Service to then ship packages, so, like I said, on our site, the average number of export markets for our—they are still tiny, microbusinesses in many cases—ended up being just under 30 per year.

Mr. BILIRAKIS. OK. In your opinion, how difficult would it be for a small business to reach the international marketplace without cross-border data flows?

Mr. BIERON. Essentially impossible. I mean, today, as we have heard, whether you are a giant, multibillion-dollar business or you are an individual who wants to send an email to somebody, at the end of the day it involves cross-border data. So, I mean, you can't get paid by somebody outside the country generally if you don't have an ability to have cross-border data flow. So it underpins, whether you are a tiny individual entrepreneur or a giant business, it underpins the way all kind of cross-border business gets done.

Mr. BILIRAKIS. Thank you.

Thank you. I yield back, Mr. Chairman. Appreciate it.

Mr. TERRY. That is all the folks that we have to ask questions, so I guess that completes our hearing today, except that all committee members, whether they were here or not, have the opportunity to submit written questions to you. I don't know if there will be any, but if there are any submitted to you, I would appreciate about a 14-day turnaround. I think that is pretty reasonable.

So with that, let's see, we do have two letters for the record. Letter on behalf of the Marketing Research Association, dated September 16, 2014, addressed to the ranking member and myself.

Then the second one is a letter on behalf of the International Affairs Division of the U.S. Chamber of Commerce dated April 3, 2014, addressed to the Office of Science and Technology Policy. Unanimous consent to submit those. No objection, so ordered.

[The information follows:]



September 16, 2014

Hon. Lee Terry (R-NE-02)
Chairman
Commerce. Manufacturing & Trade
Subcommittee

Hon. Jan Schakowsky (D-IL-09)
Ranking Member
Commerce. Manufacturing & Trade
Subcommittee

Re: Tomorrow's hearing on "Cross Border Data Flows: Could Foreign Protectionism Hurt U.S. Jobs"

Dear Chairman Terry and Ranking Member Schakowsky,

On behalf of the Marketing Research Association (MRA), I write in hopes that you will take the opportunity of your Subcommittee hearing on July 24 regarding cross border data flows to focus on issues of data privacy and the cross-border data trade between the U.S. and European Union (EU), given a significant push among European officials to eliminate the U.S.-EU Safe Harbor for data transfer.

MRA, a non-profit national membership association, represents the survey, opinion and marketing research profession[1] and strives to improve research participation and quality. We are keenly focused on data privacy, since personal data is essential to the research process and our ability to deliver insights to our clients.

The 1998 European Commission's Directive on Data Protection ("Data Directive") prohibits the transfer of "personal data" to non-EU nations that do not meet the European "adequacy" standard for privacy protection. The EU Data Directive places significant restrictions on the collection, use and disclosure of personal data that prove taxing for many researchers. Despite some complaints that the U.S., unlike the EU, lacks an organized and comprehensive federal privacy law, EU privacy law is not perfectly organized either, fragmented across its member states, with each implementing the Data Directive differently.

Intentionally or not, the EU wields the Data Directive and its "adequacy" standard as an anti-competitive trade measure, discriminating against U.S. companies in digital trade because they do not deem the U.S. to have "adequate" data privacy protections. Fortunately, in addition to adopting binding corporate rules, U.S. companies can self-certify to the US Department of Commerce that they comply with the seven principles of the U.S.-EU Safe Harbor[2] and at least have some mechanism for data transfer. While it is a self-certification, the Federal Trade Commission (FTC) enforces compliance with the Safe Harbor under its Section 5 authority to prosecute deceptive practices (not living up to one's public claims), which they have done with dozens of companies this year.

The EU is attempting to rewrite their Data Directive into a much more expansive regulation, including potential multi-million dollar liability for minimal data security breaches and prosecution of U.S. companies directly by EU authorities. Most importantly, drafters seek to renegotiate or eliminate the Safe Harbor. While kinks in their legislative process have kicked the rewrite into at least 2015, it is imperative that the U.S. maintain the Safe

[1] The research profession is a multi-billion dollar worldwide industry, comprised of pollsters and government, public opinion, academic and goods and services researchers, whose members range from large multinational corporations and small businesses to academic institutes, non-profit organizations and government agencies.

[2] Notice, Choice, Onward Transfer (to Third Parties), Access, Security, Data Integrity and Enforcement. http://export.gov/safeharbor/eu/index.asp

Marketing Research Association
1156 15th St, NW, Suite 302, Washington, DC 20005 • Ph: (202) 570-7312 • Fax: (888) 512-1050
Website: http://www.marketingresearch.org • Email: howard.fienberg@marketingresearch.org

Harbor – our primary protection for the conduct of digital commerce and research. Paul Nemitz, director of fundamental rights and European citizenship for the European Commission and one of the lead EU trade negotiators, has admitted that the move to kill the Safe Harbor "has a protectionist function."[3]

Of course, defending our interests is good, but advancing our interests is better. Comprehensive data privacy proposals have been advanced for the last few years by the FTC, the White House, and Members of Congress. All of them hope to better emulate the EU privacy regime in hopes that the US will be deemed "adequate" in its privacy protections by the EU.

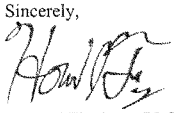
While MRA supports some form of baseline consumer data privacy law, the expansive measures envisioned by some actors go far beyond the baseline – with questionable promise of success. "Harmonization" of U.S. law to an EU standard may not make the most sense economically. As outlined by several large technology companies' chief privacy officers at an Internet Association panel discussion on March 5, 2013, innovative data businesses generally develop and grow in the US, not in Europe, and our approach to data privacy may be a key factor in our competitive advantage.[4]

More importantly, over the course of many public and private engagements in the last couple of years, Members of the European Parliament and European Commission have indicated that none of the comprehensive U.S. proposals offered so far would, if enacted, win the U.S. the coveted "adequacy" designation by the EU. It is possible that nothing short of a complete substitution of EU law for US law would satisfy EU authorities.

MRA asks that you consider the importance of "harmonization" of the U.S. and EU privacy regimes as a part of this hearing, but not in the traditional way that the term is used. There may be great value to both sides of the Atlantic in bringing our privacy approaches closer together. However, the concept of harmonization should focus more on modeling EU law after the strong enforcement mechanisms and self-regulation of the US. American trade negotiators should charge ahead with such a mandate.

We look forward to the Subcommittee's hearing tomorrow and hope you will address the importance of maintaining the U.S.-EU Safe Harbor and the potential for harmonizing EU data privacy law to a more entrepreneurial approach.

Sincerely,



Howard Fienberg, PLC
Director of Government Affairs
Marketing Research Association (MRA)

[3] "Digital Trans-Atlantic Trade: Does consumer privacy demand U.S.-EU Safe Harbor 2.0?" June 23, 2014. http://www.marketingresearch.org/news/2014/06/23/digital-trans-atlantic-trade-does-consumer-privacy-demand-us-eu-safe-harbor-20

[4] "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/news/2013/03/07/corporate-privacy-officers-discuss-global-compliance-trans-atlantic-competition-a-co

Marketing Research Association
1156 15th St, NW, Suite 302, Washington, DC 20005 • Ph: (202) 570-7312 • Fax: (888) 512-1050
Website: http://www.marketingresearch.org • Email: howard.fienberg@marketingresearch.org

CHAMBER OF COMMERCE
OF THE
UNITED STATES OF AMERICA

MYRON A. BRILLIANT
EXECUTIVE VICE PRESIDENT AND
HEAD OF INTERNATIONAL AFFAIRS

1615 H STREET NW
WASHINGTON, DC 20062-2000
202/463-5489

April 3, 2014

Mr. John P. Holdren
Assistant to the President for Science and Technology Policy
Eisenhower Executive Office Building
1650 Pennsylvania Avenue, NW
Washington, D.C. 20504

Dear Mr. Holdren:

The U.S. Chamber of Commerce, the world's largest business federation representing the interests of more than three million businesses of all sizes, sectors, and regions, as well as state and local chambers and industry associations, and dedicated to promoting, protecting, and defending America's free enterprise system, urges the U.S. government to address ongoing controversies relating to electronic surveillance by distinguishing more clearly between privacy issues associated with national security and those associated with commercial privacy practices. Further, the Chamber urges you and your colleagues in the administration to correct policymakers as well as media representatives who intentionally or mistakenly conflate the two issues, both domestically and internationally, and to reinforce advocacy for policies safeguarding cross-border digital commerce.

The Internet has revolutionized the way business is conducted and how data are used in all sectors of the global economy. Chamber members of all sectors and sizes use the Internet to interact with employees, existing and potential customers, and business partners around the world. Companies work hard to ensure that their products and services are deemed trustworthy. Companies that fail to meet customers' privacy and security expectations can expect to face swift and decisive marketplace and reputational consequences, as well as legal and regulatory enforcement consequences for regulated business sectors.

The enormous consequences of merging U.S. national security-related privacy issues and commercial privacy practices already can be felt globally. Under the

mistaken belief that U.S. businesses have conspired with the U.S. government, end users in foreign markets are either not using U.S. company services or products or are demanding that U.S.-headquartered companies needlessly place expensive servers in local markets. These types of measures have negatively affected U.S. business throughout the global marketplace, while also empowering other governments to pass rules threatening the modern, open Internet economy[1] and, in turn, thwarting one of the strongest engines of jobs, growth, and innovation.

Citizens around the world have a legitimate right to engage in a transparent discussion about privacy. In that debate, it is essential the U.S. government dispel misperceptions that are causing real competitive, reputational, and financial harm to U.S. businesses. In so doing, it is important to emphasize that U.S. companies strive to employ cutting-edge data protection and privacy measures and that concerns over government actions can only be solved by government-to-government discussions.

The Chamber believes the U.S. government must act swiftly and collaboratively to prevent the NSA controversy from undermining U.S. economic interests. These interests include, but are not limited to, the following:

- **International Trade** – Some governments are using concerns over spying as a pretext to pass misguided rules that either threaten to cut off the international flow of information or require localized servers and storage. Some of these rules are good faith attempts to address public concerns, but several governments appear to be advancing protectionist measures under the guise of national security concerns.
- **Privacy Globally** – The European Union and a number of other foreign governments are considering new approaches to data privacy. It is essential that any new rules be flexible enough to accommodate different uses and sectors.
- **Internet Governance** – The upcoming meeting of the International Telecommunications Union (ITU) in October and plans to transition oversight of the Internet Corporate of Assigned Names and Numbers (ICANN) have created a precarious situation for the future of the Internet. It is essential for the U.S. government to continue to guard against any efforts by foreign

[1] See e.g. recent statements from the European Union: http://ec.europa.eu/commission_2010-2014/kroes/en/content/making-europe-natural-home-safe-cloud-computing and Brazil: http://www.usatoday.com/story/cybertruth/2013/11/15/snowden-fallout-brazil-calls-for-local-data-storage/3588861/.

governments to use the NSA controversy as justification to upend the current, successful multi-stakeholder governance model under which the Internet has heretofore thrived.[2]

- **Data-Driven Innovation** – Data are being used for a variety of innovative new purposes, including health care, science, education, and human rights. The potential for continued increases in economic vibrancy and public benefits must not only be allowed to continue, but encouraged and facilitated. Although the White House has announced a new focus on "big data,"[3] the U.S. government must ensure that the effort is transparent and inclusive, ensuring stakeholders are informed of any long-term plans and involved in every stage of the process.
- **Commercial Privacy Practices** – Given that governments and businesses use data in very distinct ways, with vastly different privacy implications, the NSA controversy must not be allowed to rush any examination of how the private-sector collects, uses, and protects consumer information. A distinction must be made between government collection and use of data, —backed by the inherent power of its authority—with no opt-out available and commercial privacy practices, where there are marketplace curbs on bad behavior and, for some business sectors, legal and regulatory requirements to safeguard consumer data. Experience with the Internet shows that no one knows with certainty what course it will take as technology and business models evolve; therefore, policymakers must carefully consider the economic consequences of hindering the development and use of the Internet before making rash changes to consumer privacy laws or regulations.
- **Cybersecurity** – The NSA controversy has chilled progress on Capitol Hill of vital information-sharing legislation. The Chamber commends the National Institute of Standards and Technologies for collaborating with industry to create the Framework for Improving Critical Infrastructure Cybersecurity, which was released in February. The Chamber urges similar leadership by the administration and Congress to enable greater information sharing about sophisticated threats to businesses' cybersecurity. Industry still needs legislation that includes robust protections (e.g., legal liability and regulations) for businesses that voluntarily exchange information with their peers and

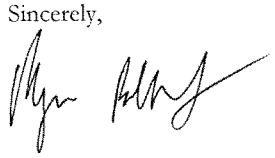
---

[2] See generally http://europa.eu/rapid/press-release_IP-14-142_en.htm.
[3] http://www.whitehouse.gov/blog/2014/01/23/big-data-and-future-privacy.

government partners. Such safeguards can coexist with protections for privacy and civil liberties.

Today's Internet and the data-driven economy, which affect businesses of all sizes and sectors, have been an enormous source of economic growth and job creation around the globe. It is unfortunate that concerns regarding revelations of U.S. national security and law enforcement activities are being used to justify actions that jeopardize the tremendous innovation in technologies and services central to the robust recovery of the U.S. economy. To nurture this immense engine of growth, the Chamber urges you and all policymakers to advocate for sound policies that ensure the free flow of data internationally and to be more outspoken in ensuring the separation of national security-related privacy issues from commercial privacy practices. The Chamber looks forward to working with you on these issues domestically and abroad.

Sincerely,



Myron Brilliant

cc: Members of the United States Congress

Mr. TERRY. And that concludes our hearing. Thank you very much.

[Whereupon, at 3:05 p.m., the committee was adjourned.]

[Material submitted for inclusion in the record follows:]

PREPARED STATEMENT OF HON. HENRY A. WAXMAN

Today's hearing is on efforts to limit the electronic movement of information across national boundaries.

The United States leads the world in technological innovation. Digital trade-related exports totaled more than $350 billion in 2011, up from about $280 billion in 2007.

In today's heavily digital commercial environment, cross-border data flows are not just a normal part of doing business, but also essential to the innovative capacity of U.S. enterprises. Any limits on international trade, including digital trade, will have an effect on the American economy and American jobs. Recent industry reports find that the efforts of foreign countries to restrict data flows—or even the threat to do so—can hurt American businesses.

There is no doubt that foreign trust in the United States Government and of U.S.-based companies has been hurt by revelations since last year about the NSA's online surveillance programs.

But other factors are also at work. Just like Americans, citizens of other nations are concerned about the massive amount of personal information being collected by private companies and whether this information is secure. In Europe, for example, the efforts to limit private data mining and to ensure basic data security protections began long before Mr. Snowden's name was known.

For example, in 2012, an Austrian law student sparked outrage in Europe over his discovery that Facebook possessed files of personal information on individual users that were hundreds of pages long. Even earlier, several European countries took action against Google's Street View service after it was revealed that Google's Street View cars collected personal information as they drove through the streets.

One way to help alleviate those fears and build trust is for the United States to establish effective baseline privacy and data security protections. That is why I have supported, and continue to support, efforts to establish such protections for consumers' information.

Regaining the trust of consumers worldwide is crucial to the continued growth of Internet and communications technology sector in the United States. That requires a multi-faceted approach—through appropriate legislation and regulation, as well as through trade negotiations and other administration efforts to prevent harmful restrictions on cross-border data flows.

I look forward to the witnesses' testimony and to our discussion today of this important topic. Thank you.

FRED UPTON, MICHIGAN
CHAIRMAN

HENRY A. WAXMAN, CALIFORNIA
RANKING MEMBER

ONE HUNDRED THIRTEENTH 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

December 19, 2014

Ms. Linda Dempsey
Vice President
International Economic Affairs
National Association of Manufacturers
733 10th Street, N.W., Suite 700
Washington, D.C. 20001

Ms. Dempsey,

Thank you for appearing before the Subcommittee on Commerce, Manufacturing, and Trade on Wednesday, September 17, 2014 to testify at the hearing entitled "Cross Border Data Flows: Could Foreign Protectionism Hurt 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, January 5, 2015. Your responses should be e-mailed to the Legislative Clerk in Word format at **Kirby.Howard@mail.house.gov** and mailed to Kirby Howard, Legislative Clerk, Committee on Energy and Commerce, 2125 Rayburn House Office Building, Washington, D.C. 20515.

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

Sincerely,

Lee Terry
Chairman
Subcommittee on Commerce,
Manufacturing, and Trade

cc: Jan Schakowsky, Ranking Member, Subcommittee on Commerce, Manufacturing, and Trade
Attachment

Linda Menghetti Dempsey, Vice President, International Economic Affairs
National Association of Manufacturers
January 9, 2015

Additional Questions for the Record: Responses

The Honorable Lee Terry

1. **From NAM's perspective, what does an effective trade policy for cross-border data transfers look like, and how does it support U.S. manufacturing?**

An effective and pro-manufacturing U.S. trade policy for cross-border data transfers would encompass four main attributes:

- The modernization and passage of new Trade Promotion Authority (TPA) legislation that would direct U.S. negotiators to ensure that governments not implement trade-related measures that impede digital trade in goods, services, restrict cross-border data flows or require local information technology storage or processing of data. The Bipartisan Congressional Trade Priorities Act of 2014 (H.R. 3830) included strong provisions regarding this issue that should be included in new legislation to be introduced this year.
- The negotiation of new trade and investment agreements, including the Trans-Pacific Partnership (TPP), Transatlantic Trade and Investment Partnership (TTIP) and the Trade in Services Agreement (TISA) that contain binding commitments to allow manufacturers and other industries to transfer, access, process or store information across borders; prohibit the imposition of restrictions that would require the establishment or use of local servers generally or as a condition of access to the market; and ensure non-discriminatory treatment of digital products and services.
- Active work by U.S. government officials to prevent the adoption of new provisions by foreign governments that would impede cross-border data flows, including work to educate other government, identify such measures as part of the annual trade barriers reports and use other tools to ensure that such provisions do not impede commerce.
- Use of trade agreement enforcement tools by the U.S. government when foreign governments violate commitments made not to restrict cross-border data flows or not to require the localization of information technology infrastructure, such as updating eligibility criteria for preference programs, including potentially the Generalized System of Preferences and the African Growth and Opportunity Act (AGOA) to ensure countries' commitment to creating a strong enabling environment for digital trade.

Such a policy would advance opportunities for manufacturers in the United States to increase exports and sales overseas. As explained in my written testimony, international trade and investment are highly important to provide manufacturers in the United States access to new customers overseas and to increase sales in a highly challenging global economy. Increasingly, manufacturers are using digital platforms, including sharing data and information across borders, to expand sales overseas, and creating new products that create new demand that is served by growing manufacturing and jobs domestically. A strong U.S. trade policy that actively addresses this issue of growing importance is important for manufacturers of all sizes in the United States.

2. The Internet of Things has dominated recent headlines and in your testimony you discuss "machine-to-machine" technologies. How are manufacturers utilizing "machine-to-machine" technology today?

As noted in my written testimony, manufacturers are at the forefront of building "machine to machine" technologies (M2M or the Internet of Things (IOT)) to transfer data remotely between machines and other systems. In 2013, the market for IOT was estimated to be worth $1.3 trillion, by 2020, the market is expected to be worth $3.04 trillion by 2020 according to market research firm IDC.[1]

As explained in "How Smart Connected Products are Transforming Competition:"

> Embedded sensors, processors, software, and connectivity in products (in effects, computers are being put inside products), coupled with a product cloud in which product data is stored and analyzed and some applications are run, are driving dramatic improvements in product functionality and performance. Massive amounts of new product usage data enable many of those improvements.[2]

Among the many ways that manufacturers are using M2M and IOT technology include:

- Increasing industrial automation through sensors, controllers and other information technologies.
- Using global positioning software (GPS) to locate lost devices, navigate and track machinery.
- Maximize user safety in hazardous locations by enabling remote control of machinery (*e.g.*, monitor and control mining machinery from control room above mines).
- Coordinate and optimize activities and tasks among multiple machines working towards a common purpose by analyzing data from each component in the systems (e.g., farm tractors, backhoes, tillers, and other farming equipment working in sync to maximize the output of the farm (grain, produce, etc.) with the minimum input (water, fertilizer, etc.)).
- Deliver over-the-air (OTA) software updates remotely to improve the productivity or address maintenance issues for a wide range of consumer and industrial products that are M2M enabled.
- Reduce equipment downtime and increase utilization of assets by analyzing performance usage data to identify potential issues and address them proactively (*e.g.*, measuring equipment temperature or vibrations remotely leads to proactive maintenance visit to avoid product failure).
- Offering consumers and businesses innovative products and services powered through the cloud.

---

[1] Stephen McBride, "IoT Market to Reach $3.04 trn by 2020," **ITP.NET** (Nov. 14, 2014), accessed at http://www.itp.net/600792-iot-market-to-reach-304trn-by-2020-idc.

[2] Michael E. Porter & James E. Heppelmann, "How Smart, Connected Products are Transforming Competition," **Harvard Business Review** (Nov. 2014), accessed at http://www.ptc.com/File%20Library/Topics/Harvard%20Business%20Review/HBR_How-Smart-Connected-Products-Are-Transforming-Competition.pdf.

More specifically, data captured from embedded sensors, software and processors enable manufacturers to gather and exchange information on product usage, performance and environment that can be leveraged to improve a variety of manufacturer's value chain activities:

- Product design:
  - Leverage data collected from the product to design better performing and higher quality products (*e.g.*, remove features customers do not use, increase ease of use of existing features, identify root-cause of component failure).
- Marketing and sales:
  - Improve market segmentation by analyzing usage data to create a better understanding of how the product is used to provide features and services specifically tailored to different customer segments, and deliver ongoing services or improve product performance (*e.g.*, automatic replenishment of spare parts or consumables to avoid product downtime; continuously update and improve products through remote software upgrades and configurations).
  - Change business models to offer usage-based billing or product as a service, selling the utility of the product instead of the fixed asset.
  - Extend product offering to include products and services powered through the cloud.
- Manufacturing processes:
  - Increase efficiency of the factory floor through smart connected factories – automating manufacturing processes.
- Service:
  - Improve existing service efficiency through remote service, predictive and preventive maintenance, improved parts management and efficient field service (*e.g.*, utilizing real-time and historical failure, performance and maintenance history data collected from all products sold, manufacturers can predict product failure and proactively fix the issue before the product actually fails, preventing costly product or production downtime.
  - Optimize warranty contracts – leverage data collected from the product to prevent warranty issues, identify breach in warranty by end-use monitoring, and update and adjust warranty contracts based on how customers are actually using the product.
  - Provide value-added services, by extending the product offering beyond the physical product to include additional services in which the customer may be interested based on product-usage data.
- Logistics:
  - Use technology to track and monitor shipments in real time, which is especially important for agriculture, food, medical and pharmaceutical and other time-sensitive products.

In developing and utilizing these technologies, manufacturers work to ensure that the privacy and security of information collected and transmitted by such by including safeguards at the beginning of the design process

a. Are those uses threatened when foreign governments place commercial restrictions on data flows?

Government restrictions on cross-border data flows and limitations on the locations of information technology infrastructure severely undermine the ability of manufacturers to make use of these technologies and to compete successfully in foreign markets. In particular, such limitations prevent the aggregation, sharing and analysis of information developed in different countries that could be used to enhance product development, usage, maintenance or access to customers. Such restrictions also add additional costs, limiting the ability of manufacturers to allocate resources most efficiently and effectively. Such restrictions also add additional capital costs in the form of servers and other data storing infrastructure to partition and secure data based on foreign regulations to ensure compliance, limiting the ability of manufacturers to allocate resources most efficiently and effectively. Such restrictions can also prevent companies from shipping products to certain jurisdictions. That is why we also need to be diligent so U.S. government actions do not unnecessarily prompt reaction abroad that could impact data flows and avoid circumstances that cause countries to impose restrictions on cross-border data flows because of those actions.

The US International Trade Commission's 2014 report on *Digital Trade in the US and Global Economies, Part 2* estimated that removing barriers to digital trade would increase U.S. real GDP by up to $41 billion and employment by up to 400,000 full-time equivalent positions.[3]

In order to prevent artificial restrictions on the deployment and adoption of IOT, we recommend that the TPA and future trade agreements include binding provisions to limit any regulations to specific policy objectives and that are done so in a manner that is nondiscriminatory and are not trade restrictive.

b. Have these restrictions, or proposed regulations, discouraged adoption of "machine-to-machine" technologies?

While the development of M2M, IOT and cloud technologies have created new opportunities, government initiatives that restrict cross-border data flows and require the localization of information technology infrastructure have a chilling effect on manufacturers' use of these technologies and inhibits many of the opportunities to optimize product development, marketing and sales as well as service activities that benefit both the manufacturer and the end user discussed previously on an international scale. While M2M and IOT technologies might be deployed in some geographical markets, some manufacturers have been hesitant to put in the most advanced technologies in countries where such restrictions are imposed or threatened due to the complexity and high cost of compliance.

3. The U.S. is engaged in several major trade negotiations including TPP, TTIP, and TiSA. How can previous agreements guide the ongoing trade negotiations with respect to cross-border data flows?

Over the last decade, U.S.-negotiated trade agreements have increasingly dealt with digital and electronic commerce issues as technology has increasingly become part of how trade is conducted. As restrictions on cross-border data flows started to arise, more recent trade agreements have started to tackle this issue more precisely, most significantly in the Korea-U.S. Free Trade

[3] U.S. International Trade Commission, "Digital Trade in the U.S. and Global Economies Part 2," Publ. No. 4485, Inv. 332-540 (August 2014), accessed at http://www.usitc.gov/publications/332/pub4485.pdf.

Agreement (KORUS FTA), which included general language indicating that the Parties should not impose restrictions on cross-border data flows as well as specific language limiting the use of such restrictions related to financial data.

As noted in my written testimony, the importance of ensuring cross-border data flows has also been dealt with in several multilateral agreements and initiatives, including in the Asia Pacific Economic Cooperation (APEC) forum's "Digital Prosperity Checklist" (2008), the APEC Innovation Principles (2011), the APEC Privacy Framework (2012), the Organization for Economic Cooperation and Development (OECD) Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data" (July 2013) and U.S.-EU Information and Communication Technology (ICT) Principles (2011).

While much work has been done recognizing the issue, creating new, binding and enforceable legal obligations in trade agreements is needed to address fully the types of barriers that are arising, as specified in my written testimony

4. Is it fair to say that previous trade agreements recognizing the importance of the free flow of data have supported the development and growth of industries critical to the U.S. economy and jobs, such as manufacturing?

Prior trade agreements have been very important to growing manufacturing in the United States. By reducing barriers, requiring fair treatment of U.S. products, services and investments, and promoting adequate and effective protection of intellectual property rights, U.S. free trade agreements (FTA) have been critical drivers of increased exports and sales by manufacturers and other businesses to our FTA partners. America's 20 existing trade agreement partners account for less than 10 percent of the global economy but purchase nearly half of all U.S. manufactured goods exports. By improving provisions on cross-border data flows in future trade agreements, the competitiveness of America's manufacturers and other businesses will be further enhanced in overseas markets.

5. Your testimony mentioned that world trade in manufactured goods expanded from $4.8 trillion in 2000 to $11.5 trillion in 2012. How much of this expansion would you attribute to advancements in information and communication technologies?

As explained in my written testimony and during the hearing, the increased ability of manufacturers in the United States to export has been substantially aided by the advancements and utilization of information and communications technologies (ICT). The use of ICT had been shown to increase productivity in the U.S. economy and has a particularly powerful effect on small and medium sized enterprises (SMEs) and their ability to export.

For example, a 2013 study by the Boston Consulting Group (BCG) showed that tech-savvy small and medium-sized enterprises (SMEs) create more new jobs and drive more revenue gains than SMEs using little technology, and are far more likely to have international customers. BCG estimates that if more SMEs in the United States employed the full range of available IT tools, including basic productivity software, Internet connectivity and new Cloud-based services, these

businesses could inject an additional $357 billion into the economy and hire 2.1 million more employees.[4]

While data are not available on the specific impact of ICT technologies on the growth of manufacturing exports in particular, it is useful to note that the increase in manufacturing trade coincides with the growth of the Internet's role throughout the economy. For example, according to the U.S. Census Bureau, 52 percent of U.S. manufacturers' shipments were associated with e-commerce in 2012, compared with just 18 percent in 2000.[5]

a. Do you believe these same advancements played a role in the U.S. producing a record high $1.38 trillion in manufactured goods in 2013? If so, how?

Yes, the advancement and utilization of ICT technologies and cross-border data flows has had and will continue to have an important positive impact on manufacturing exports. In particular, the utilization of such technologies has enabled manufacturers to compete more successfully in a tough global economy by lowering costs, improving efficiencies and to growth product, supply and distribution networks more effectively overseas. From utilizing cloud computing to provide an internet storefront or data flows to manage a global production network or improving an end product's capability through Internet and data flow enabled software updates, manufacturers are increasingly using ICT and data flows to make better products more efficiently and to reach directly consumers around the country and the world.

The Honorable Jerry McNerney

6. You suggested that issues related to data flow should be included in trade agreements. What form should this take – privacy, openness, security, IT?

New trade agreements should build upon existing provisions related to digital trade and include new and binding commitments to allow manufacturers and other industries to transfer, access, process or store information across borders; prohibit the imposition of restrictions that would require the establishment or use of local servers generally or as a condition of access to the market; and ensure non-discriminatory treatment of digital products and services. In including such provisions, it is important to ensure that any regulations on cross-border data flows and related issues:

1) Be limited to specific and legitimate public policy objectives, consistent with international treaties;
2) Be established pursuant to transparent procedures allowing comment by all interested parties;
3) Not constitute unnecessary barriers to trade in services;
4) Take into account and not seek to supplant competitive market forces that are already achieving regulatory objectives.

---

[4] See, e.g., **Boosting Exports, Jobs and Economic Growth by Expanding the ITA**, Information Technology & Innovation Foundation (March 2012), accessed at http://www2.itif.org/2012-boosting-exports-jobs-expanding-ita.pdf; **Ahead of the Curve**, Boston Consulting Group (Oct. 5, 2013), accessed at https://www.bcgperspectives.com/content/articles/technology_software_globalization_ahead_curve_lessons_technology_growth_small_business_leaders/.

[5] U.S. Census Bureau, accessed at http://www.census.gov/econ/estats/2012/all2012tables.html.

FRED UPTON, MICHIGAN
CHAIRMAN

HENRY A. WAXMAN, CALIFORNIA
RANKING MEMBER

ONE HUNDRED THIRTEENTH 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

December 19, 2014

Mr. Brian Bieron
Executive Director
Global Public Policy
eBay Incorporated
1250 I Street N.W., Suite 1200
Washington, D.C. 20005

Mr. Bieron,

Thank you for appearing before the Subcommittee on Commerce, Manufacturing, and Trade on Wednesday, September 17, 2014 to testify at the hearing entitled "Cross Border Data Flows: Could Foreign Protectionism Hurt 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, January 5, 2015. Your responses should be e-mailed to the Legislative Clerk in Word format at **Kirby.Howard@mail.house.gov** and mailed to Kirby Howard, Legislative Clerk, Committee on Energy and Commerce, 2125 Rayburn House Office Building, Washington, D.C. 20515.

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

Sincerely,

Lee Terry
Chairman
Subcommittee on Commerce,
Manufacturing, and Trade

cc: Jan Schakowsky, Ranking Member, Subcommittee on Commerce, Manufacturing, and Trade
Attachment

Subcommittee on Commerce, Manufacturing, and Trade
Cross Border Data Flows: Could Foreign Protectionism Hurt U.S. Jobs?
Response to Questions Submitted for the Record:
Mr. Brian Bieron, Executive Director, Global Public Policy, eBay Incorporated

Additional Questions for the Record

The Honorable Lee Terry

In your testimony, you mention that G20 countries are responsible for 65% of these protectionist policies. How can the ongoing trade negotiations, including TPP, the U.S.-E.U. Safe Harbor, TTIP, and TiSA, improve the marketplace for small businesses that use the eBay Marketplace?

Trade negotiations can remove barriers that currently inhibit technology-enabled small businesses from selling across borders. The US is currently involved in several negotiations that can serve to reduce barriers to trade. Each negotiation has unique issues that it could potentially address:

TPP

Small businesses face challenges when navigating and complying with trade laws around the world, and must dedicate their limited resources to compliance costs that are proportionally higher for their smaller size. Technology-enabled small businesses, in particular, confront complex customs procedures that complicate access to the international marketplace. Many small businesseses avoid selling internationally all together because of confusing customs procedures. The TPP can help to resolve this issue for small businesses by raising and harmonizing the de minimis thresholds of all negotiating parties. The de minimis threshold is the monetary level below which an importer is exempted from customs duty and paperwork requirements. De minimis levels can be quite low in TPP nations; for example the de minimis in Canada is just $20.

The TPP Customs chapter would be the ideal location for codifying a de minimis level for all TPP parties. Moreover, the TPP will be the first trade agreement to have an intense focus on improving the global supply chain, and raising de minimis would fit perfectly into that overarching method. Increasing the de minimis threshold would benefit small businesses by reducing customs and shipping burdens. Increased thresholds would improve access to the global supply chain. Also, as retailers integrate an e-commerce presence into their business model, it's important to break down barriers to low-cost goods for consumers.

In the US, eBay supports the Low Value Shipment Regulatory Modernization Act (S. 489/H.R. 970). This legislation would increase the US de minimis level from $200 to $800. The legislation also includes a Sense of Congress that US trade negotiators should seek similar commitments from our trading partner nations to ensure that the international marketplace is open to US exports. We advocate that an $800 de minimis threshold should be codified in the Customs chapter of the TPP to create an open marketplace for technology-enabled small businesses.

TTIP

The TTIP negotiations are timely, and present a unique opportunity to create rules and principles for today's and tomorrow's trade. With the characteristics of the new trade as our starting point, this section makes specific proposals for what we believe should be included within the three broad areas identified as the pillars of a TTIP agreement.

Break new ground on customs relief thresholds

Under the *de minimis* rule in the US and the customs relief thresholds in the EU, products less than $200 and €150 respectively are exempt from customs duties. By raising that threshold to $1,000 dollar/€800, trade generated by micro and small businesses would receive a significant boost as cost, paperwork and delays would be reduced for exporting SMEs.[i] The TTIP should include a commitment to a minimum threshold of $1,000 dollar/€800; this baseline level could be linked it to the consumer price index. This level should be applicable regardless of country of origin. Creating a baseline *de minimis* level between the EU and the US and where the aim is to have such a baseline level adopted by other trading partners would support small business to fully take part in the global economy.

Support cross-border delivery services through partnerships

Micro and small businesses in particular rely on postal systems for cross border shipping services. This often means that they miss out on important services such as tracking; that the service is perceived as unreliable by consumers; and, that it is expensive relative to the service level and delivery time. The European Commission recently published the results of a survey[ii] among SMEs and "transport of goods" was mentioned as one of the most burdensome policy areas for both EU and non-EU SMEs. Shipping solutions as those proposed below are often overlooked in trade negotiations even though they are integral to supporting the participation in trade small businesses and consumers.

The TTIP could:

- Create harmonised rules for EU and US postal operators to deal with damaged packages, tracking requirements and data requirements. The objective is to make it simpler for small businesses to manage the intricacies of transatlantic and global trade.
- Create interoperable tracking systems.
- Become an instrument for strengthening the links between services of commercial courier companies and postal operators on both sides of the Atlantic. We believe in partnerships between postal operators and express carriers for the development of the type of delivery services small businesses and their customers demand (e.g. end-to-end tracking; standardized return solutions; affordable, sufficiently fast and reliable services).
- Encourage creating tools to improve customer knowledge about the nature of EU and US postal services.

Trusted trader schemes for micro and small businesses

The US and the EU have signed a decision on the mutual recognition of their respective trusted trader program: the Customs-Trade Partnership Against Terrorism (C-TPAT) program in the U.S. and the Authorized Economic Operator (AEO) program in the EU. Reciprocal implementation is effective since 31 January 2013.

This is a welcome development which the TTIP should build on by:

- The TTIP should extend the scope beyond (i) safety and security to cover also customs simplification and (ii) manufacturers and exporters to cover also all other operators in the supply chain.
- The TTIP negotiations should explore how to ensure that micro and small businesses can participate and benefit from a transatlantic trusted trader scheme. To the extent that micro and small businesses are dissuaded from joining the AEO and C-TPAT programs[iii], the TTIP should put in place mechanisms that would have the effect of linking those businesses to those programs, e.g. through the use of intermediary authorized operators.
- The TTIP negotiations could be used to set up an eCustoms project similar to the ITAIDE[iv] but focused on micro and small businesses and developing practical customs solutions for seamless transatlantic trade and adapted to their needs and resources (ITAIDE runs "Living Labs", which are pilots centered around large European exporters in four different sectors.)

Web-enabled micro and small firms exporting have a very different risk profile to large corporations. Our research shows that, compared to traditional firms, they export to several countries; they trade in several product categories; and the export pattern is generally infrequent.[v] In the context of investigating and ensuring small businesses' participation in transatlantic trusted trader scheme, the TTIP negotiations should investigate what new types of data and data sources (including corporate sources) should inform risk assessment as well as compliance with trusted trader criteria.

TISA

The International Services Agreement should ensure an open and competitive environment for e-commerce to thrive. It should include provisions that allow users to access and use services, applications, and devices of their choice. It should make permanent, and strengthen, the 1998 WTO e-commerce moratorium in which WTO members committed to the practice of not imposing customs duties on electronic transmissions. Moreover, TISA should create strong, binding, rules that support the cross-border flow of data and bar forced localization requirements including requirements for the building of local infrastructure in order to offer services. It should include Internet intermediary liability protections, for providers online platforms, designed to ensure that intermediaries are not treated as publishers of content, exclusive of criminal law, communications privacy law, and intellectual property claim. Such a provision will encourage innovation and the development of new types of cross border services. Finally, TISA should mandate the concept of technological neutrality, so that all technologies are given an equal chance to compete in the marketplace.

The Honorable Jerry McNerney

You mentioned that U.S. leadership in data flow is key. How do you envision this: internal policy, trade policy, or other?

The US must adopt smart policies in domestic legislation and regulation as well as in the trade context in order to maintain its leadership stake in the digital arena. In terms of domestic policy, the US should avoid any outright restrictions on data transfers, onerous licensing requirements that

might inhibit the growth of new digital services, and taxation of digital transmissions. In the trade context, the US should create enforceable rules against localization requirements for digital service providers, onerous customs requirements that effectively inhibit digital transmissions that support physical goods, and seek out interoperable privacy regimes that protect citizens' sense of dignity while enabling data-based innovation.

---

[i] This is a proposal put forward also by the National Board of Trade in their report 2013:4 (available: http://www.kommers.se/publikationer/Rapporter/2013/Global-Value-Chains-and-the-Transatlantic-Trade-and-Investment-Partnership-/); by the World Economic Forum in their 2013 report "Enabling Trade" (available: http://www3.weforum.org/docs/WEF_SCT_EnablingTrade_Report_2013.pdf); and in a summary report by the OECD (available at http://www.oecd.org/trade/tradedev/IBD2013Report.pdf)

[ii] Avalable at: http://www.ebaymainstreet.com/news-events/european-commission-publishes-list-top-barriers-small-businesses-eu

[iii] National Board of Trade makes the following remark in their report 2013:4 "Global Value Chains and the Transatlantic Trade and Investment Partnership": "*Recent improvements in trade logistics, such as 'authorized economic operators' and other trusted trader programs, also typically benefit large economic actors.*" Likewise, World Economic Forum suggests in their 2013 report "Enabling Trade": "*For example, one relatively straightforward policy [...] is to ensure that initiatives to reduce regulatory compliance such as trusted trader programmes are open to smaller firms*".

[iv] www.itaide.org

[v] The National Board of Trade describes the characteristics of e-traders as (1) selling into a large number of markets simultaneously, (2) seldom established in the markets they sell into, (3) small, and (4) often shipping a large number of small consignments rather than single big ones. (Report 2012:4 "E-Commerce: New Opportunities, New Barriers)

FRED UPTON, MICHIGAN
CHAIRMAN

HENRY A. WAXMAN, CALIFORNIA
RANKING MEMBER

ONE HUNDRED THIRTEENTH 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

December 19, 2014

Mr. Sean Heather
Vice President
Center for Global Regulatory Cooperation
U.S. Chamber of Commerce
1615 H Street N.W.
Washington, D.C. 20062

Mr. Heather,

Thank you for appearing before the Subcommittee on Commerce, Manufacturing, and Trade on Wednesday, September 17, 2014 to testify at the hearing entitled "Cross Border Data Flows: Could Foreign Protectionism Hurt 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, January 5, 2015. Your responses should be e-mailed to the Legislative Clerk in Word format at **Kirby.Howard@mail.house.gov** and mailed to Kirby Howard, Legislative Clerk, Committee on Energy and Commerce, 2125 Rayburn House Office Building, Washington, D.C. 20515.

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

Sincerely,

Lee Terry
Chairman
Subcommittee on Commerce,
Manufacturing, and Trade

cc: Jan Schakowsky, Ranking Member, Subcommittee on Commerce, Manufacturing, and Trade
Attachment

CHAMBER OF COMMERCE
OF THE
UNITED STATES OF AMERICA

SEAN HEATHER
VICE PRESIDENT
CENTER FOR GLOBAL REGULATORY
COOPERATION

1615 H STREET, N.W.
WASHINGTON, D.C. 20062-2000
202/463-5368

January 8, 2015

Kirby Howard
Legislative Clerk
Committee on Energy and Commerce
2125 Rayburn House Office Building
Washington, D.C. 20515

Dear Mr. Howard,

The Chamber appreciates the opportunity to have appeared before the Subcommittee on Commerce, Manufacturing, and Trade back in September to testify at the hearing entitled "Cross Border Data Flows: Could Foreign Protectionism Hurt U.S. Jobs?" As requested, please find attached the Chamber's response to the questions I received to be submitted for the record.

Sincerely,

[redacted]

Sean Heather
Vice President
Center for Global Regulatory Cooperation
U.S. Chamber of Commerce

Chamber Responses to Questions for the Record

1. From the Chamber's perspective, what does an effective trade policy for cross-border data transfers look like and how does it support U.S. industry?

   An effective trade policy requires a two pronged approach. The first prong should be USTR securing strong commitments in trade agreements that bar forced localization efforts by governments that prevent the cross-border flow of data. Further, commitments in trade agreements must also include data transfer mechanisms that facilitate the movement of data while addressing legitimate privacy concerns.

   More specifically, trade agreement provisions should address the ability to freely transfer data by: (1) an expressed commitment to allowing cross-border data transfers; (2) a prohibition on data localization requirements; and (3) a non-exhaustive list of data transfer mechanisms. Trade agreement provisions should also meaningfully limit the public policy exemptions allowed under the General Agreement in Services (GATS) Article XIV, by requiring any transfer prohibitions to be no more trade restrictive than necessary. Most importantly, these provisions need to be binding and enforceable, with minimal exceptions for non-conforming measures.

   The second prong to an effective trade policy in support of cross-border data transfers is to engage bilaterally with countries outside of trade negotiations as various problematic regulatory proposals arise. A coordinated effort between various U.S. government agencies as well as Embassy staff on the ground is often needed to overly broad, misguided, and protectionist approaches proposed by foreign governments. In the past year, such measures have been proposed in more than a dozen countries. This trend is likely to continue and a whole-of-government response will be needed for the foreseeable future to meet these challenges head on.

2. How do existing restrictions on cross-border data flows impact consumers and end-users?

   Restrictions on cross-border data flows deprive consumers of valuable products and services and raise costs. The restrictions serve to take the "world" out of the World Wide Web, severely limiting the potential of the Internet to serve as an engine of growth in the United States and worldwide. Some good examples can be found in the case studies illustrated in the joint U.S. Chamber of Commerce/Hunton & Williams study: *Business without Borders: The Importance of Cross-Border Data Transfers to Global Prosperity.*[1]

[1] See Section III, available at https://www.uschamber.com/sites/default/files/021384_BusinessWOBorders_final.pdf.

3. What will policy makers need to consider to maintain U.S. competitiveness and ensure that the benefits of cross-border data flows lead to the creation of more U.S. jobs and domestic investment?

   U.S. policy makers need to better appreciate and be prepared to respond to the continued fallout generated from the NSA-related surveillance allegations. Foreign governments have used these allegations an excuse to win political points or to promote local champions and some governments, including Germany's, have passed laws related to government procurement that bar market access to U.S. companies. The inability or unwillingness of policymakers to distinguish policy measures designed to address government use of data versus commercial use of data is arguably the single biggest threat to cross-border data flows and our competitiveness.

4. There are multiple, ongoing trade negotiations between the U.S. and major trade partners including the TPP, the U.S.-E.U. Safe Harbor, TTIP, and TiSA. In these negotiations how important is it for the countries engaged to reach agreement on cross-border data flow principles?

   It is very important for each of the negotiations mentioned above to commit governments to strong rules; and those rules must be binding, enforceable and with limited non-conforming measures in order for the agreements to be effective. The Chamber would add the negotiation with China over a bilateral investment treaty to the list of negotiations where the interests of preserving cross-border data flows must be appropriately addressed. It is difficult to imagine how any of these negotiations could equip American business to be competitive in a digital age without these provisions.

   a. Are there examples in other trade agreements that the U.S. can look to for guidance in this process?

      A number of trade agreements have acknowledged the significance of cross-border data transfers to the global economy as a fundamental tenet of the agreement. For example, Article 14.5 of the U.S.-Panama Trade Promotion Agreement highlights the importance of helping small and medium-sized enterprises "overcome obstacles" that impede their participation in electronic commerce and maintaining "cross-border data flows of information as an essential element in fostering a vibrant environment for electronic commerce."

      Similarly, Article 15.8 of the United States-Korea Free Trade Agreement (KORUS) recognizes "the importance of the free flow of information in facilitating trade" and pushes the parties to the agreement to "refrain from imposing or maintaining unnecessary barriers to electronic information flows across borders."

However, these agreements are lacking because the commitments are merely aspirational. Without binding and enforceable language our trading partners are free to disregard any data flows language.

The KORUS agreement also has more specific language in the financial services chapter, but South Korea is interpreting the language extremely narrowly and not providing proper allowances regarding the transferring and processing of data. Moreover, the KORUS language is limited to one chapter.

Moving forward, trade negotiators need to advance concrete commitments, and cross-border data flow provisions must apply to all sectors.

b. I understand over 3000 companies rely on the U.S.-E.U. Safe Harbor Framework to transfer data between the trade zones. How important is a functioning Safe Harbor Framework to your members?

A functioning U.S.-EU Safe Harbor is extremely important to these companies and their clients when conducting businesses across the Atlantic. Companies from many sectors and sizes rely on this data transfer mechanism to conduct both routine operational functions and to interact with clients while abiding by trusted, well-established data protection methods. A well-functioning U.S-EU Safe Harbor is not only critical bilaterally, but also can serve as a model data transfer mechanism for other trading partners.

While we are encouraged by the discussions between the U.S. and EU regulators, we believe it is important that proposed revisions to the framework be tailored in response to identified, actual problems. Policymakers must avoid temptations to raise hypotheticals or concerns unrelated to commercial use of data. If not, the viability of the U.S.-EU Safe Harbor as a data transfer mechanism will be in jeopardy.

