

This is a preliminary transcript of a Committee hearing. It has not yet been subject to a review process to ensure that the statements within are appropriately attributed to the witness or member of Congress who made them, to determine whether there are any inconsistencies between the statement within and what was actually said at the proceeding, or to make any other corrections to ensure the accuracy of the record.

RPTS RULL

DCMN CRYSTAL

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, D.C.

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.

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

Staff Present: Leighton Brown, Press Assistant; Graham Dufault, Policy Coordinator, CMT; Melissa Froelich, Counsel, CMT; Kirby Howard, Legislative Clerk; Paul Nagle, Chief Counsel, CMT;

Michelle Ash, Minority General Counsel; and Lisa Goldman, Minority 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.

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 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. I have 1 minute, if anybody wants it.

Gentleman from Texas.

[The prepared statement of Mr. Terry follows:]

***** COMMITTEE INSERT *****

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.

[The prepared statement of Mr. Olson follows:]

***** COMMITTEE INSERT *****

Mr. Terry. I recognize the gentlelady from 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 -- okay. And I would like to yield to Mr. McNerney whatever time is left.

[The prepared statement of Ms. Schakowsky follows:]

***** COMMITTEE INSERT *****

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.

[The prepared statement of Mr. McNerney follows:]

***** COMMITTEE INSERT *****

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.

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 cochaired 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.

[The prepared statement of Ms. Blackburn follows:]

***** COMMITTEE INSERT *****

Mr. Terry. Mr. Guthrie, statement?

Mr. Bilirakis.

Mr. Bilirakis. No. Thank you.

Mr. Terry. All time being yield 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 -- 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, SENIOR DIRECTOR, EBAY, INC. PUBLIC POLICY LAB; SEAN HEATHER, VICE PRESIDENT, CENTER FOR GLOBAL REGULATORY COOPERATION, EXECUTIVE DIRECTOR, INTERNATIONAL POLICY & ANTITRUST POLICY, U.S. CHAMBER OF COMMERCE; AND LAURA K. DONOHUE, PROFESSOR OF LAW, GEORGETOWN UNIVERSITY LAW CENTER, DIRECTOR, CENTER ON NATIONAL SECURITY AND THE LAW

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.

Mr. Terry. Thank you.

[The prepared statement of Ms. Dempsey follows:]

***** INSERT 1-1 *****

Mr. Terry. 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 mid-sized 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 mid-sized 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 mid-sized 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 mid-sized 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.

Mr. Terry. Thank you, Mr. Bieron.

[The prepared statement of Mr. Bieron follows:]

***** INSERT 1-2 *****

Mr. Terry. 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 compete 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 become 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 1/3 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.

Mr. Terry. Thank you, Professor.

[The prepared statement of Ms. Donohue follows:]

***** INSERT 1-3 *****

Mr. Terry. Mr. Heather, you are now recognized for 5 minutes.

STATEMENT OF SEAN 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.

Mr. Terry. Thank you, Mr. Heather.

[The prepared statement of Mr. Heather follows:]

***** INSERT 1-4 *****

Mr. Terry. 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. Okay.

Mr. Bieron.

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 2X 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. Yeah. 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 curbed 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. Okay. 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 are proceeding was -- 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. Okay. 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.

[The information follows:]

***** COMMITTEE INSERT *****

Mr. Bieron. 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 -- and 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. Yeah. Yeah.

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. Yeah. 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. Okay. 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's 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, micro businesses in many cases -- ended up being just under 30 per year.

RPTS BAKER

DCMN CRYSTAL

[3:05 p.m.]

Mr. Bilirakis. Okay. 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.

[The information follows:]

***** COMMITTEE INSERT *****

Mr. Terry. 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:]

***** COMMITTEE INSERT *****

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

[Whereupon, at 3:07 p.m., the committee was adjourned.]