EXAMINING THE EU SAFE HARBOR DECISION AND IMPACTS FOR TRANSATLANTIC DATA FLOWS

JOINT HEARING

BEFORE THE

SUBCOMMITTEE ON COMMERCE, MANUFACTURING, AND TRADE

AND THE

SUBCOMMITTEE ON COMMUNICATIONS AND TECHNOLOGY

OF THE

COMMITTEE ON ENERGY AND COMMERCE

HOUSE OF REPRESENTATIVES

ONE HUNDRED FOURTEENTH CONGRESS

FIRST SESSION

NOVEMBER 3, 2015

Serial No. 114–97

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

U.S. GOVERNMENT PUBLISHING OFFICE

99–571 WASHINGTON : 2016

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

COMMITTEE ON ENERGY AND COMMERCE

FRED UPTON, Michigan
Chairman

JOE BARTON, Texas
Chairman Emeritus
ED WHITFIELD, Kentucky
JOHN SHIMKUS, Illinois
JOSEPH R. PITTS, Pennsylvania
GREG WALDEN, Oregon
TIM MURPHY, Pennsylvania
MICHAEL C. BURGESS, Texas
MARSHA BLACKBURN, Tennessee
Vice Chairman
STEVE SCALISE, Louisiana
ROBERT E. LATTA, Ohio
CATHY MCMORRIS RODGERS, Washington
GREGG HARPER, Mississippi
LEONARD LANCE, New Jersey
BRETT GUTHRIE, Kentucky
PETE OLSON, Texas
DAVID B. MCKINLEY, West Virginia
MIKE POMPEO, Kansas
ADAM KINZINGER, Illinois
H. MORGAN GRIFFITH, Virginia
GUS M. BILIRAKIS, Florida
BILL JOHNSON, Missouri
BILLY LONG, Missouri
RENEE L. ELLMERS, North Carolina
LARRY BUCSHON, Indiana
BILL FLORES, Texas
SUSAN W. BROOKS, Indiana
MARKWAYNE MULLIN, Oklahoma
RICHARD HUDSON, North Carolina
CHRIS COLLINS, New York
KEVIN CRAMER, North Dakota

FRANK PALLONE, JR., New Jersey
Ranking Member
BOBBY L. RUSH, Illinois
ANNA G. ESHOO, California
ELIOT L. ENGEL, New York
GENE GREEN, Texas
DIANA DEGETTE, Colorado
LOIS CAPPS, California
MICHAEL F. DOYLE, Pennsylvania
JANICE D. SCHAKOWSKY, Illinois
G.K. BUTTERFIELD, North Carolina
DORIS O. MATSUI, California
KATHY CASTOR, Florida
JOHN P. SARBANES, Maryland
JERRY MCNERNEY, California
PETER WELCH, Vermont
BEN RAY LUJAN, New Mexico
PAUL TONKO, New York
JOHN A. YARMUTH, Kentucky
YVETTE D. CLARKE, New York
DAVID LOEBSACK, Iowa
KURT SCHRADER, Oregon
JOSEPH P. KENNEDY, III, Massachusetts
TONY CARDENAS, California

SUBCOMMITTEE ON COMMERCE, MANUFACTURING, AND TRADE

MICHAEL C. BURGESS, Texas
Chairman

LEONARD LANCE, New Jersey
Vice Chairman
MARSHA BLACKBURN, Tennessee
GREGG HARPER, Mississippi
BRETT GUTHRIE, Kentucky
PETE OLSON, Texas
MIKE POMPEO, Kansas
ADAM KINZINGER, Illinois
GUS M. BILIRAKIS, Florida
SUSAN W. BROOKS, Indiana
MARKWAYNE MULLIN, Oklahoma
FRED UPTON, Michigan *(ex officio)*

JANICE D. SCHAKOWSKY, Illinois
Ranking Member
YVETTE D. CLARKE, New York
JOSEPH P. KENNEDY, III, Massachusetts
TONY CÁRDENAS, California
BOBBY L. RUSH, Illinois
G.K. BUTTERFIELD, North Carolina
PETER WELCH, Vermont
FRANK PALLONE, JR., New Jersey *(ex officio)*

SUBCOMMITTEE ON COMMUNICATIONS AND TECHNOLOGY

GREG WALDEN, Oregon
Chairman

ROBERT E. LATTA, Ohio
Vice Chairman
JOHN SHIMKUS, Illinois
MARSHA BLACKBURN, Tennessee
STEVE SCALISE, Louisiana
LEONARD LANCE, New Jersey
BRETT GUTHRIE, Kentucky
PETE OLSON, Texas
MIKE POMPEO, Kansas
ADAM KINZINGER, Illinois
GUS M. BILIRAKIS, Florida
BILL JOHNSON, Missouri
BILLY LONG, Missouri
RENEE L. ELLMERS, North Carolina
CHRIS COLLINS, New York
KEVIN CRAMER, North Dakota
JOE BARTON, Texas
FRED UPTON, Michigan *(ex officio)*

ANNA G. ESHOO, California
Ranking Member
MICHAEL F. DOYLE, Pennsylvania
PETER WELCH, Vermont
JOHN A. YARMUTH, Kentucky
YVETTE D. CLARKE, New York
DAVID LOEBSACK, Iowa
BOBBY L. RUSH, Illinois
DIANA DEGETTE, Colorado
G.K. BUTTERFIELD, North Carolina
DORIS O. MATSUI, California
JERRY MCNERNEY, California
BEN RAY LUJÁN, New Mexico
FRANK PALLONE, JR., New Jersey *(ex officio)*

CONTENTS

[1] Available at: *http://docs.house.gov/meetings/if/if16/20151103/104148/hhrg-114-if16-20151103-sd015.pdf.*

EXAMINING THE EU SAFE HARBOR DECISION AND IMPACTS FOR TRANSATLANTIC DATA FLOWS

TUESDAY, NOVEMBER 3, 2015

HOUSE OF REPRESENTATIVES,
SUBCOMMITTEE ON COMMERCE, MANUFACTURING, AND TRADE,
JOINT WITH THE
SUBCOMMITTEE ON COMMUNICATIONS AND TECHNOLOGY,
COMMITTEE ON ENERGY AND COMMERCE,
Washington, DC.

The subcommittees met, pursuant to call, at 10:00 a.m., in room 2123, Rayburn House Office Building, Hon. Michael Burgess (chairman of the subcommittee on Commerce, Manufacturing, and Trade) presiding.

Present from the subcommittee on Commerce, Manufacturing, and Trade: Representatives Burgess, Lance, Blackburn, Harper, Guthrie, Olson, Pompeo, Kinzinger, Bilirakis, Brooks, Mullin, Upton (ex officio), Schakowsky, Clarke, Kennedy, Welch, and Pallone (ex officio).

Present from the subcommittee on Communications and Technology: Representatives Walden, Latta, Shimkus, Blackburn, Lance, Guthrie, Olson, Pompeo, Kinzinger, Bilirakis, Johnson, Long, Collins, Barton, Upton (ex officio), Eshoo, Welch, Clarke, Loebsack, Matsui, McNerney, and Pallone (ex officio).

Staff present: Gary Andres, Staff Director; Ray Baum, Senior Policy Advisor for Communications and Technology; Leighton Brown, Press Assistant; James Decker, Policy Coordinator for Commerce, Manufacturing, and Trade; Andy Duberstein, Deputy Press Secretary; Melissa Froelich, Counsel for Commerce, Manufacturing, and Trade; Grace Koh, Counsel for Telecom; Paul Nagle, Chief Counsel for Commerce, Manufacturing, and Trade; Tim Pataki, Professional Staff Member; David Redl, Counsel for Telecom; Charlotte Savercool, Professional Staff for Communications and Technology; Dylan Vorbach, Legislative Clerk for Commerce, Manufacturing, and Trade; Gregory Watson, Legislative Clerk for Communications and Technology and Oversight and Investigations; Michelle Ash, Chief Counsel for Commerce, Manufacturing, and Trade; Christine Brennan, Press Secretary; Jeff Carroll, Staff Director; David Goldman, Chief Counsel for Communications and Technology; Lisa Goldman, Counsel; Tiffany Guarascio, Deputy Staff Director and Chief Health Advisor; Lori Maarbjerg, FCC Detailee; Diana Rudd, Legal Fellow; Ryan Skukowski, Policy Ana-

lyst; and Jerry Leverich, Counsel for Communications and Technology.

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

Mr. BURGESS. Very well. I will ask all of our guests to take their seats. The joint subcommittees on Commerce, Manufacturing, and Trade and the subcommittee on Communications and Technology will now come to order.

I will recognize myself 4 minutes for the purpose of an opening statement.

And I do want to welcome you all to our joint hearing on the Transatlantic Data Flows and the Impact of the European Union Safe Harbor Decision.

Over 4,400 businesses have self-certified compliance with the Safe Harbor agreement through the Department of Commerce. A lot of jobs, a lot of industries are connected to those 4,400 businesses. The Safe Harbor agreement has provided a mechanism to carry out commerce with the European Union. There is no trade partnership, no trade partnership that is more important than the trade partnership with the European Union. The depth and breadth of the United States and the European Union relationship is not simply economic. It is strategically important, and it is also one of respect and cooperation.

In today's world, as our members know, you can't do business without digital data flows. So today, our two subcommittees send an important message. There is no reason to delay. Both sides have all that is needed to put a sustainable Safe Harbor agreement into place. It is our understanding that there is an agreement in principle. And I certainly thank the important work that the Department of Commerce has done to achieve a new agreement. They offered a bipartisan briefing to our members. Their message was the correct one. We cannot let anything get in the way of moving as quickly as possible to secure the new Safe Harbor agreement.

I also want to thank the important enforcement work that the Federal Trade Commission has done enforcing the existing Safe Harbor framework. I know that they will continue to do the same for the new Safe Harbor.

For the sake of our jobs, for the sake of small and medium-sized businesses relying on the Safe Harbor, and of all of the jobs that they support in both the United States and the European Union, I encourage all parties to stay at the negotiating table to solidify a new data transfer agreement well in advance of the January 2016 deadline. There is no other path forward. And I can assure you that our committee will continue to watch the negotiations closely and to be helpful where we can.

[The prepared statement of Mr. Burgess follows:]

PREPARED STATEMENT OF HON. MICHAEL C. BURGESS

Over 4,400 businesses self-certified compliance with the Safe Harbor agreement through the Department of Commerce. An awful lot of jobs and an awful lot of industries are connected to those 4,400 businesses.

The Safe Harbor Agreement had provided a safe mechanism to carryout commerce with the European Union. There is no trade partnership more important than the trade partnership with the EU. The depth and breadth of the U.S. and EU relation-

ship is not simply economic—this is a strategically important relationship of respect and cooperation. But in today's world, as our members know, you can't do business without digital data flows.

So today, our two subcommittees send an important message. There is no reason to delay. Both sides have all that is needed to put a sustainable Safe Harbor agreement in place. Our understanding is that there is an agreement in principle. And I applaud the important work the Department of Commerce has done to achieve a new agreement. They offered a bi-partisan briefing to our Members last week. Their message is the right one—we cannot let anything get in the way of moving as quickly as possible to secure the new Safe Harbor agreement. I also want to applaud the important enforcement work that the Federal Trade Commission has done enforcing the existing safe harbor framework. I know that they will do the same for the new safe harbor.

For the sake of the small and medium sized business relying on the Safe Harbor, and all of the jobs they support in both the U.S. and the EU, I encourage all parties to stay at the negotiating table to solidify a new data transfer agreement well in advance of the January 2016 deadline. There is no other path forward that I can support. And I can assure you that our Committee will continue to watch the negotiations closely.

Mr. BURGESS. I would now like to recognize the vice chair of the Communications subcommittee, Mr. Latta, for the remainder of the time.

Mr. LATTA. Well, I thank the chairman for yielding, and I also thank our witnesses for being here today.

We are all aware of the crucial role the internet plays in the trade relationship between the United States and the European Union. For over a decade, the U.S.-E.U. Safe Harbor agreement has recognized the internet's importance and kept cross-border data flows open to reduce barriers to trade.

However, since the Court of Justice ruled the agreement invalid, the U.S. has diligently worked on revising the framework to prevent a hindrance to the global economy. My hope for today's hearing is to continue the discussion on a framework that will provide marketplace stability and adequately protect consumer data. It is imperative for U.S. and European companies to be able to operate and conduct transatlantic business with certainty.

And with that, Mr. Chairman, I yield back the balance of my time.

Mr. BURGESS. The chair thanks the gentleman. The gentleman yields back.

The chair recognizes the ranking member of the Subcommittee on Commerce, Manufacturing, and Trade, Ms. Schakowsky, for 4 minutes for an opening statement, please.

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

Ms. SCHAKOWSKY. Thank you, Mr. Chairman, and Chairman Walden as well for calling today's joint hearing on the implications of the Schrems v. Data Protection Commissioner decision on the Safe Harbor agreement and the future of U.S.-E.U. cross-border data flows. This is an important and timely subject for our subcommittee to consider, and I welcome our witnesses.

The Safe Harbor framework included principles that U.S. companies could follow in order to meet E.U. standards for data security and privacy. That framework has enabled American companies to attract and retain European business with the American and E.U.

economies representing almost half of the global economic activity, the value of a functional Safe Harbor agreement cannot be overstated.

The Schrems decision threatens to undermine business between our countries and the European continent. The more than 4,000 American companies and millions of U.S. employees who have worked to abide by the Safe Harbor agreement cannot afford that outcome.

But the Schrems decision does rightly call into question the adequacy of U.S. data security practices. There are legitimate concerns about the protection of personal information collected and stored online, not just for European citizens, but actually for our own as well.

As a former member of the House Intelligence Committee, I believe that we must establish adequate and transparent data security and privacy protections, and if we fail to do that, the economic implications could be disastrous.

I will soon introduce legislation that would require strong security standards for a wide array of personal data, including geolocation, health-related, biometric, and email and social media account information. It would also require breached companies to report the breach to consumers within 30 days. My bill would enhance data security standards here at home, and it would probably have the added benefit of making the E.U. more confident in U.S. privacy and data security standards.

I look forward to hearing our witnesses' prescriptions for a path forward that will maintain cross-border data flows, while enhancing the security of data held in the United States. Our businesses, our workers and consumers in the United States and European Union deserve no less.

And I would like to yield the balance of my time to Representative Matsui for her remarks.

Ms. MATSUI. Thank you. Thank you very much.

Data is a lifeblood of the 21st century economy and critical to innovation and competition. Through my work as co-chair of the Congressional High Tech Caucus, I understand the importance of cross-border flow policies that support economic growth.

This is about more than the over 4,000 businesses which rely on Safe Harbor but also the hundreds of millions of consumers in the United States and Europe that rely upon services that move data across borders. We can all agree that the Safe Harbor standards written before the advent of the smartphone or the widespread use of cloud services deserve to be updated, and we can do so in a way that recognizes the importance of protecting private personal information while also reaping the benefits of our interconnected economies.

I look forward to hearing from today's witnesses, and I yield back the balance of my time.

Ms. SCHAKOWSKY. And I yield back.

Mr. BURGESS. The chair thanks the gentlelady. The gentlelady yields back.

The chair now recognizes the chairman of the full committee, Mr. Upton, 4 minutes for an opening statement, please.

OPENING STATEMENT OF HON. FRED UPTON, A REPRESENTATIVE IN CONGRESS FROM THE STATE OF MICHIGAN

Mr. UPTON. Well, thank you, Mr. Chairman.

Our partnership with Europe has always been marked by friendship, shared interest, and mutual benefit. From autos to ideas, an awful lot of things made in Michigan and across the country have made their way across the Atlantic.

Of course, it is just not the U.S. that benefits from our relationship with Europe. The exchange of goods and services between the U.S. and E.U. amounts to almost $700 billion. It is critical to both of our economies. Important to this trade infrastructure is the free flow of information, and the inability to pass data freely between the two jurisdictions is a barrier to the growth of our two economies.

So we must move swiftly towards a framework for a sustainable Safe Harbor. And while I recognize there are some who want to leverage this important relationship and focus on areas of disagreement, I would urge folks to keep in mind the countless small and medium enterprises that rely on the Safe Harbor framework. I support the work and direction of the Department of Commerce in negotiating this new framework and I encourage its speedy adoption, and yield the balance of my time to Mrs. Blackburn.

[The prepared statement of Mr. Upton follows:]

PREPARED STATEMENT OF THE HON. FRED UPTON

Our partnership with Europe has always been marked by friendship, shared interest, and mutual benefit. From autos to ideas, an awful lot of things made in Michigan have made their way across the Atlantic. Of course, it's not just Michigan that benefits from our relationship with Europe. The exchange of goods and services between the U.S. and the EU amounts to almost 700 billion dollars; it is critical to both of our economies. Integral to this trade infrastructure is the free flow of information, and the inability to pass data freely between the two jurisdictions is a barrier to the growth of our two economies.

We must move swiftly forward toward a framework for a sustainable Safe Harbor. While I recognize that there are some who want to leverage this important relationship and focus on areas of disagreement, I would urge folks to keep in mind the countless small and medium enterprises that rely on the Safe Harbor framework. I support the work and direction of the Department of Commerce in negotiating this new framework and I encourage its speedy adoption.

Mrs. BLACKBURN. Thank you, Mr. Chairman.

And I am so appreciative of our witnesses being here and for the hearing on this issue today. It is something that needs some thoughtful attention, and we look forward to directing our attention to solving the issue.

The chairman mentioned the amount of trade, and when you are looking at nearly $1 trillion in bilateral trade and knowing that the free flow of information is important to this, data transfer rights are important to this discussion. We do need to approach this thoughtfully.

Mr. Meltzer, I was caught by your stat on digital trade and what it has done to increase the U.S. GDP, and then on the fact that the U.S.-E.U. data transfers are 50 percent higher than the U.S.-Asia transfers, and I think that the difference in those flows is really quite remarkable. So I will want to visit with you more about that.

Congress has attempted, through a couple of pieces of legislation, as you all know, the Judicial Redress Act and the Freedom Act, to address the privacy concerns. I had the opportunity several months ago to be in Europe and discuss with some of our colleagues, Members of Parliament, their concerns, and I hope that we are going to be able to negotiate in good faith and find some answers.

And with that, Mr. Chairman, I will yield to you the balance of my time if any other Member would like to claim it.

Mr. BURGESS. The chair thanks the gentlelady. The gentlelady yields back.

The chair recognizes the gentlelady from California, Ms. Eshoo, the ranking member of the subcommittee on Communications.

OPENING STATEMENT OF HON. ANNA G. ESHOO, A REPRESENTATIVE IN CONGRESS FROM THE STATE OF CALIFORNIA

Ms. ESHOO. Thank you, Mr. Chairman.

And I want to thank you and the ranking member of your subcommittee for joining with Communications and Technology Subcommittee to have this important hearing. I thank the witnesses for being here. And we have a very full hearing room, so there is not only a great deal of interest in this issue, but there is a lot at stake.

In my Silicon Valley congressional district and on both sides of the Atlantic, companies continue to reel from the October 6 decision by the European Court of Justice to nullify the U.S.-E.U. Safe Harbor agreement. As one expert remarked, "aside from taking an ax to the undersea fiberoptic cables connecting Europe to the United States, it is hard to imagine a more disruptive action to the transatlantic digital commerce."

For the past 15 years, thousands of companies, as has been stated by, I think, every member that has spoken so far, both small and large have relied upon this agreement to effectively and efficiently transfer data across the Atlantic and in a manner that protected consumer privacy.

Recognizing the magnitude of the court's decision, earlier this month I joined with several colleagues, both sides of the aisle, and a letter to Secretary Pritzker and the FTC Chairwoman Ramirez urging the Administration to redouble their efforts to come up with a new agreement with the E.U.

Given the strong economic relationship between the U.S. and E.U., estimated over $1 trillion annually, $1 trillion, I mean that is—you are really talking about something when you say $1 trillion—we have to move quickly with the European regulators to provide a swift solution to what is no doubt creating a great deal of uncertainty. In practice, this means reaching the Safe Harbor 2.0 agreement as soon as possible.

I also think we have to acknowledge that there is an elephant in the room, which is a major contributing factor in my view in the court's ruling: privacy concerns relating to U.S. surveillance methods. Having served on the House Intelligence Committee for nearly a decade, I have consistently worried about the impact of U.S. surveillance activities on both U.S. citizens and companies. Given that the E.U.'s court decision made clear that the U.S. must provide "an

adequate level of protection" for E.U.-U.S. data transfers, I look forward to hearing from our witnesses about how this can be achieved in the Safe Harbor 2.0.

I think if we don't really deal with this, we will be missing a large point here. In a digital economy, there is nothing more important than the free flow of data across borders. A Congress that is united in support of this goal and the reinstatement of a new agreement I think will ensure the continued growth of digital commerce in the years to come.

So I thank our witnesses for being here today and for your commitment to ensuring unfettered data transfers between the U.S. and the E.U.

And with that, I yield back the balance of my time, Mr. Chairman. Thank you.

Mr. BURGESS. The gentlelady yields back. The chair thanks the gentlelady.

The chair recognizes the chairman of the Communications and Technology Subcommittee, Mr. Walden, for 4 minutes for an opening statement.

OPENING STATEMENT OF HON. GREG WALDEN, A REPRESENTATIVE IN CONGRESS FROM THE STATE OF OREGON

Mr. WALDEN. Thank you, Mr. Chairman. And I want to thank our witnesses for being here. This is obviously an issue of great importance to all of us.

The borderless nature of the internet is an important force driving economic success and innovation. For internet-based companies, the value of free flow of digital data between the E.U. and the United States is obvious. But analysts have also pointed out that up to 75 percent of the value added by transnational data flows on the internet goes to traditional industries, especially via increases in global growth, productivity, and employment.

Communications and technology underpin every sector of the global economy, from precision farming to sensor-monitored shipping, from Facebook to McDonald's, from footwear manufacturers to custom furniture makers. These networks are the infrastructure of the 21st century economy, and free flow of information is critical to making that infrastructure work.

The free flow of information has especially benefited small and medium-sized companies by opening markets on both sides of the Atlantic that were previously inaccessible. These are the businesses that gain new consumers simply by virtue of the nearly costless ability to find new suppliers, strike quicker agreements, or access new markets. These are the businesses that will suffer the greatest harm and bear the greatest risk if we are not able to come to a new Safe Harbor framework.

The Safe Harbor cut down on the cost of compliance with the various state privacy regulations in the European Union. Without the shelter of a Safe Harbor, these businesses have the choice of operating at increased risk, paying expensive costs to lower that risk, or simply stopping the flow of information altogether, that is, stopping business altogether.

The Department of Commerce estimates that in 2013, 60 percent of the 4,000-plus participants in the Safe Harbor framework were

small or medium-sized enterprises, spanning 102 different industry sectors. A break in the flow of data has the potential to cause real impacts to the economies on both sides of the proverbial pond.

So I am encouraged to hear that the negotiators on Safe Harbor 2.0 have reached an agreement in principle—that is really good news—and I cannot emphasize enough how important it is to reach a new and firm agreement before the grace period elapses in January.

I would like to thank our witnesses again for spending time to discuss their understanding of the impact of the ruling of the European Court of Justice. We welcome your thoughts and let forward to hearing from you.

With that, I would yield such time as the—pardon me? Oh, I guess Mr. Barton didn't want any time. Thank you. So I yield back balance of my time.

[The prepared statement of Mr. Walden follows:]

PREPARED STATEMENT OF THE HON. GREG WALDEN

The borderless nature of the Internet is an important force driving economic success and innovation. For Internet-based companies, the value of the free flow of digital data between the EU and the US is obvious. But analysts have also pointed out that up to 75 percent of the value added by transnational data flows on the Internet goes to "traditional" industries, especially via increases in global growth, productivity, and employment. Communications and technology underpin every sector of the global economy—from precision farming to sensor-monitored shipping, from Facebook to McDonald's, from footwear manufacturers to custom furniture makers. These networks are the infrastructure of the 21st century economy and the free flow of information is critical to making that infrastructure work.

The free flow of information has especially benefited small and medium-sized enterprises by opening markets on both sides of the Atlantic that were previously inaccessible. These are the businesses that gained new consumers simply by virtue of the nearly costless ability to find new suppliers, strike quicker agreements, or access new markets. These are the businesses that will suffer the greatest harm and bear the greatest risk if we are not able to come to a new Safe Harbor framework. The Safe Harbor cut down on the cost of compliance with the various state privacy regulations in the European Union. Without the shelter of a Safe Harbor, these businesses have the choice of operating at increased risk, paying expensive costs to lower that risk, or simply stopping the flow of information altogether—that is, stopping business altogether.

The Department of Commerce estimates that in 2013, 60 percent of the 4,000-plus participants in the Safe Harbor framework were small or medium-sized enterprises, spanning 102 different industry sectors. A break in the flow of data has the potential to cause real impacts to the economies on both sides of the proverbial pond. I am encouraged to hear that the negotiators on Safe Harbor 2.0 have reached an "agreement in principle," and I cannot emphasize enough how important it is to reach a new and firm agreement before the grace period elapses in January.

Mr. BURGESS. The chair thanks the gentleman. The gentleman yields back.

The chair recognizes the ranking member of the full committee, Mr. Pallone of New Jersey, 4 minutes for an opening statement, please.

OPENING STATEMENT OF HON. FRANK PALLONE, JR., A REPRESENTATIVE IN CONGRESS FROM THE STATE OF NEW JERSEY

Mr. PALLONE. Thank you, Mr. Chairman.

This is the committee's second hearing on the topic of data moving across national borders. The digital movement of data affects

consumers and businesses in both the United States and in Europe and in every country of the world.

The U.S. leads the world in technological innovation. It has exported over $380 billion worth of digital services in 2012. Meanwhile, internet commerce grew threefold from 2011 to 2013 and is expected to reach 133 billion by 2018. And the economic relationship between the United States and the European Union is the strongest in the world.

Since our December 2014 hearing on this issue, the big change is that the European Court of Justice invalidated the Safe Harbor agreement between the United States and the European Union that allowed American companies to transfer European users' information to the U.S., and the elimination of the Safe Harbor has caused great uncertainty.

However, as early as 2013, long before the court's October 2015 decision, the 15-year-old agreement was under renegotiation. And during this time, the U.S. and the E.U. have been working hard to strengthen the privacy principles of the original agreement to ensure they cover the newest business models and data transfers that exist.

Almost a year later, we today repeat our desire to see those negotiations completed. I urge the parties to quickly finalize a new agreement tailor-made for the modern economy and the modern consumer. A new agreement can and should improve consumer privacy and data security. Businesses can and should adhere to strong privacy principles from inception.

Building trust with consumers worldwide requires a multifaceted approach through appropriate legislation and regulation, as well as through trade negotiations, and therefore, I also would urge this Congress to act by passing effective baseline privacy and data security protections. For the internet of the future, economic gains and consumer protections go hand-in-hand. When consumers feel safe that their personal information is protected, they do more business online.

I hope that today's discussion, as well as the ongoing negotiations between the United States and the E.U. will encourage a step in the right direction on data privacy not only for Europeans but for American citizens as well. We can have innovation and protections for consumer privacy. We have done it time and time again. There is no reason why it should be different in this space than in any other.

In today's heavily digital commercial environment, cross-border data flows are not just a normal part of doing business but essential to the American economy and American jobs. And I welcome this opportunity, Mr. Chairman, to discuss the value of secure and free data flow between the United States and Europe.

I yield back.

[The prepared statement of Mr. Pallone follows:]

PREPARED STATEMENT OF HON. FRANK PALLONE, JR.

Thank you, Mr. Chairman. This is the Committee's second hearing on the topic of data moving across national borders. The digital movement of data affects consumers and businesses in both the United States and in Europe, and in every country of the world.

The United States leads the world in technological innovation. It has exported over $380 billion worth of digital services in 2012. Meanwhile, Internet commerce grew threefold from 2011 to 2013 and is expected to reach $133 billion by 2018. And the economic relationship between the United States and European Union is the strongest in the world.

Since our December 2014 hearing on this issue, the big change is that the European Court of Justice invalidated the Safe Harbor agreement between the United States and the European Union that allowed American companies to transfer European users' information to the U.S. The elimination of the Safe Harbor has caused great uncertainty.

However, as early as 2013, long before the Court's October 2015 decision, the 15-year old agreement was under renegotiation. During this time, the U.S. and E.U. have been working hard to strengthen the privacy principles of the original agreement to ensure they cover the newest business models and data transfers that exist.

Almost a year later, we today repeat our desire to see those negotiations completed. I urge the parties to quickly finalize a new agreement tailor-made for the modern economy and the modern consumer.

A new agreement can and should improve consumer privacy and data security. Businesses can and should adhere to strong privacy principles from inception.

Building trust with consumers worldwide requires a multifaceted approach through appropriate legislation and regulation, as well as through trade negotiations. Therefore, I also would urge this Congress to act by passing effective baseline privacy and data security protections. For the Internet of the future, economic gains and consumer protections go hand-in-hand. When consumers feel safe-that their personal information is protected-they do more business online.

I hope that today's discussion, as well as the ongoing negotiations between the U.S. and E.U. will encourage a step in the right direction on data privacy not only for Europeans, but for American citizens as well. We can have innovation and protections for consumer privacy. We have done it time and time again. There is no reason why it should be different in this space than in any other.

In today's heavily digital commercial environment, cross-border data flows are not just a normal part of doing business, but essential to the American economy and American jobs.

I welcome this opportunity to discuss the value of secure and free data flow between the United States and Europe.

Thank you, I yield back.

Mr. BURGESS. The gentleman yields back. The chair thanks the gentleman for his comments.

This concludes Member opening statements. The chair would remind Members that pursuant to committee rules, all Members' opening statements will be made part of the record.

And we do want to thank our witnesses for being here today, for taking time to testify before the subcommittee. You will each have an opportunity to give an opening statement. That will be followed by a round of questions from Members.

Our panel for today's hearing will include Ms. Victoria Espinel, President and CEO of the Business Software Alliance; Mr. Joshua Meltzer, Senior Fellow for Global Economy and Development at the Brookings Institute; Mr. Marc Rotenberg, President of the Electronic Privacy Information Center; and Mr. John Murphy, Senior Vice President for International Policy at the United States Chamber Of Commerce.

We appreciate all of you being here with us today. We will begin the panel with you, Ms. Espinel, and you are recognized for 5 minutes for a summary of your opening statement.

STATEMENTS OF VICTORIA ESPINEL, PRESIDENT AND CEO, BUSINESS SOFTWARE ALLIANCE; JOSHUA MELTZER, SENIOR FELLOW, GLOBAL ECONOMY AND DEVELOPMENT, BROOKINGS INSTITUTE; MARC ROTENBERG, PRESIDENT, ELECTRONIC PRIVACY INFORMATION CENTER; AND JOHN MURPHY, SENIOR VICE PRESIDENT FOR INTERNATIONAL POLICY, U.S. CHAMBER OF COMMERCE

STATEMENT OF VICTORIA ESPINEL

Ms. ESPINEL. Thank you very much.

Good morning, Chairman Burgess and Ranking Member Schakowsky, Chairman Walden and Ranking Member Eshoo, and members of both subcommittees.

My name is Victoria Espinel. Thank you for the opportunity to testify today on behalf of BSA, the software alliance. BSA is the leading advocate for the global software industry in the United States and around the world.

While the 19th century was powered by steam and coal and the 20th century by electricity, cars, and computers, the 21st century runs on data. Today, data is at the core of nearly everything we touch. Banking, genome mapping, teaching our children, and safely getting home from work and back again, all run on data.

And this data economy is a global phenomenon. People around the world are benefiting from data innovation. Accordingly, we recognize that, as we proceed, we must be diligent to ensure personal privacy is fully respected and robust security measures are in place to guard the data involved.

Barriers to the free movement of data undermine the benefits of the data economy. Recent developments in Europe present a significant challenge that must be taken seriously and warrants immediate action. Last month, the European Court of Justice struck down the Safe Harbor. The Safe Harbor set out rules that enabled nearly 5,000 American companies to provide a huge array of data services to European enterprises and individuals. Companies abiding by the Safe Harbor rules could easily and efficiently transfer data to the U.S. consistent with E.U. law.

The European Court of Justice decision upended this process. The uncertainty about international data flows created by the European Court of Justice's decision deters innovation and makes it much more difficult for our members to serve their millions of customers in Europe, which harms U.S. competitiveness.

To address this, Congress and the U.S. Government should engage immediately and actively with their European counterparts to restore stability in transatlantic data flows. Specifically, we need three things. First, rapid consensus on a new agreement to replace the Safe Harbor; second, sufficient time to come into compliance with the new rules; and third, a framework in which the European Union and the United States can develop and agree on a sustainable long-term solution that reflects and advances the interests of all stakeholders.

To the first point, fortunately, the United States and the E.U. were already deep in talks to revise the Safe Harbor agreement when the European Court of Justice issued its decision. And to this

I want to join the chairman in thanking the Department of Commerce for all the hard work they have done on the negotiation far.

The new version of the framework will include up-to-date safeguards. Updating the framework makes good sense. Much has changed since the Safe Harbor was first set up in the year 2000. The volume of data is increasing exponentially. Here is an incredible fact: More than 90 percent of the data that exists in the world today was created in the last 2 years alone, and that is a rate of change that will continue to increase exponentially. The volume of business data worldwide is doubling every 15 months, so these negotiations must continue, and the new Safe Harbor must be finalized quickly.

Second, even if there is consensus on a new agreement, as we believe there will be, companies will need an appropriate standstill period in which to adapt their operations to the new legal realities. An appropriate standstill period is essential to consumers on both sides of the Atlantic.

And finally, while a new agreement to replace the Safe Harbor is a vital and immediate step, it is not the complete solution to the larger issue of privacy protections in the digital age. We urge Congress and the United States Government to look to the longer term.

The European Court of Justice ruling set a standard of essential equivalence between privacy rules in Europe and the United States, in effect, a comparative analysis of our respective regimes. The European Court of Justice points most sharply at U.S. surveillance regimes put in place to protect our national security and their impact on individual privacy. Balancing these essential goals is a task this Congress has and will continue to consider. Most recently, the enactment of the USA Freedom Act is recognition that the balance is ever-changing and laws must stay up-to-date.

Ultimately, however, essential equivalence and the pursuit of protecting privacy in a changing world will be a dynamic concept that will change as laws and practices evolve. We need a framework that is sustainable over the long term. The original Safe Harbor lasted nearly 15 years. To achieve that sort of stability, we will need to develop a more enduring solution for data transfers.

The United States and Europe are not as far apart on privacy as some might think. Where there are gaps span the Atlantic, whether perceived or actual, we can close those through a combination of dialogue and international commitments, and Congress will be a key part of enabling this to happen.

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

[The prepared statement of Ms. Espinel follows:]

Joint Hearing on

"Examining the EU Safe Harbor Decision and Impacts for Transatlantic Data Flows"

The Subcommittees on Commerce, Manufacturing, and Trade, and Communications and Technology

November 3, 2015

Washington, DC

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

Testimony of Victoria Espinel
President and CEO, BSA | The Software Alliance
Joint Hearing on "Examining the EU Safe Harbor Decision and Impacts for Transatlantic Data Flows"
November 3, 2015
Washington, DC

Good morning Chairman Burgess, and Ranking Member Schakowsky, Chairman Walden and Ranking Member Eshoo, and members of both Subcommittees. My name is Victoria Espinel, and I am the President and CEO of BSA | The Software Alliance ("BSA"). BSA is the leading advocate for the global software industry in the United States and around the world.[1]

I appreciate the opportunity to testify today on behalf of BSA. BSA has long been a strong supporter of efforts to promote and preserve free flows of data across borders.

BSA members provide a wide range of market-leading software and online services to consumers and enterprises across the globe. Billions of customers from around the world – from the smallest business and most remote farm to the largest multinational corporations – rely on our solutions to store, process and derive insights from their data, and to do business with suppliers, partners, and their own customers. In a very real sense, data is the fuel that helps businesses today compete and succeed. Cross-border data flows are therefore key to the current and future success of the United States economy. When events occur that threaten the legal underpinnings that enable such data flows, they pose great disruptions which can forestall that promise of common benefit.

The recent decision in Europe striking down the U.S.-EU Safe Harbor is thus of significant concern to us. Uncertainty about international data flows deters innovation, and makes it much more difficult for our millions of customers to do business in Europe.

Congress, and the U.S. Government more broadly, need to engage immediately and actively with their European counterparts to restore trust and efficiency to trans-Atlantic data flows. Specifically, we need three things: rapid consensus on a new agreement to replace the Safe Harbor, sufficient time to come into compliance with the new rules, and a framework in which the European Union and United States can develop and agree on a sustainable, long-term solution that reflects and advances the interests of all stakeholders.

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

The U.S.-EU Safe Harbor

As the Subcommittees are well aware, on October 6, 2015, the EU's highest court—the Court of Justice of the European Union—struck down the U.S.-EU Safe Harbor Framework.

Under EU law, personal information—which includes a very wide range of data—can generally only be moved to third countries under the cover of protections deemed "adequate" by the European Union. The U.S.-EU Safe Harbor Framework, which was adopted in 2000, was designed to allow companies to self-certify their commitment to seven specific privacy principles, and thereby demonstrate that they provide "adequate" privacy protection as required by EU law. For 15 years,

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

thousands of U.S. and European companies relied on that mechanism to do business with each other and to serve individuals and enterprises in Europe.
In striking down the Safe Harbor, the Court of Justice explained that "adequacy" requires that the protections afforded to European information when it travels *outside* of Europe must be "essentially equivalent" to the protections afforded to that information *inside* of Europe. The Court made clear that in assessing essential equivalence, it is necessary to consider a country's rules governing the storage and access of data by law enforcement, and the ability of Europeans to seek judicial redress for breaches of their privacy rights. The Court was particularly troubled by the Snowden leaks and allegations of "indiscriminate surveillance and interception" and "mass and undifferentiated accessing" of Internet users' personal data by U.S. public authorities.

The Importance of the U.S.-EU Safe Harbor on Both Shores of the Atlantic

The striking down of the Safe Harbor has created substantial legal and business uncertainty. The disruption is not a one-way street, limited in its harm to U.S. companies that do business in Europe. Many European companies that do substantial business in the United States, including pharmaceutical, aviation, and automotive firms, routinely transfer data between the United States and Europe.

At the time of the Court's decision, more than 4,000 companies were using the Safe Harbor mechanism to transfer data to the United States. This included multinational software companies, such as BSA's own members, who often move data across the Atlantic for processing or to improve the quality and efficiency of their services. But it also included American companies in a diverse range of other sectors including media, retail, leisure, consumer goods, and even agribusiness, who relied on the Safe Harbor to serve European consumers, to do business with European partners, and to make use of our world-class datacenter capabilities and innovative data analytics services. As important, following the Court of Justice's decision, European companies that could transfer data to Safe Harbored companies simply and easily may now need to comply with more burdensome rules to transfer data outside of Europe. Furthermore, while still valid, those alternative transfer mechanisms have been called into question as potentially susceptible to the same concerns as the Safe Harbor.

The invalidation of the Safe Harbor disrupts each and every one of these companies.

A 2013 study by the European Centre for International Political Economy ("ECIPE"), for example, found that in the absence of the Safe Harbor, the value of U.S. services exported to the European Union could drop by -0.2 percent to -0.5 percent.

The harm would be bilateral: EU service exports to the United States would be expected to decrease anywhere between -0.6 percent and -1 percent.[2] With U.S. imports of private commercial services totaling more than $148 billion in 2013,[3] this is not an insignificant figure.

Alternative Routes to Transfer Data

Now that the Safe Harbor has been struck down, American companies can no longer rely on it to transfer data here from the 28 countries in the European Union. However, the Court did not address any of the other EU law mechanisms that are used today to transfer data from the European Union to the United States, such as model contract clauses, or binding corporate rules.

Both the European Commission and European data protection authorities have reaffirmed that these and other EU data transfer mechanisms remain available at least for another three months following the Court's decision. This has given both companies transferring data and their customers some confidence that their data can still flow to the United States consistent with EU law in the near term.

---

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

[3] United States Trade Representative, European Union, Key Trade and Investment Data and Trends, *available online at* https://ustr.gov/countries-regions/europe-middle-east/europe/european-union.

In addition, companies transferring data, including BSA's members, continue to apply the same robust security measures to information in their care – providing further reassurance to customers.

Those alternative mechanisms are not a cure-all, however. While many companies used the Safe Harbor as part of an array of different transfer mechanisms, the Safe Harbor served a unique role as among the simplest of these mechanisms. For example, if a U.S. cloud provider does business with 100 European enterprises, prior to the Court's judgment, that cloud provider could do so through compliance with a single mechanism—the Safe Harbor. Today, that company might need to put in place a data transfer agreement with all 100 enterprises, possibly in 28 different EU markets, and potentially file or even seek regulatory approval from data protection authorities in many of these markets. That process places a heavy burden on the cloud provider, and one that can be particularly difficult for smaller companies to bear. It is also a long process as European regulatory approvals can take time, especially if many companies seek this approval simultaneously. With the invalidation of Safe Harbor, European data protection authorities face the prospect of having to process hundreds or thousands of such applications.

Also concerning, there are signs that the overall stability of the EU-U.S. framework for transferring data is threatened. Recently, for example, German data protection authorities announced that they will no longer authorize transfers to the United States on the basis of Safe Harbor, nor will they issue new authorizations for transfers to the United States under data transfer agreements or binding corporate rules. The ECIPE study that I mentioned above in fact contemplated this "worst case" scenario. It found that if the alternatives to the Safe Harbor were also unavailable, bringing data flows to a near halt, imports of services into the European Union from the United States could decrease by -16.6 percent to -24 percent.

There are also warning signs that this trend may be spreading to countries outside the European Union, many of which have adopted European-style data protection laws. Swiss authorities have now said that the U.S.-Swiss Safe Harbor, which mirrors the U.S.-EU Safe Harbor, no longer constitutes a sufficient legal basis for data transfers under Swiss law. Israel, also, has revoked authorizations for data transfers under the Safe Harbor.

Immediate Next Steps

When the Court of Justice issued its decision, the United States and European Union governments were already deep in negotiations on revising the Safe Harbor agreement. This new version of the Safe Harbor Framework will include up-to-date safeguards for "Safe Harbored" data in the United States.

Updating the Safe Harbor Framework makes good sense. Much has changed since the Safe Harbor was first agreed in 2000. Today, data is generated and transferred in quantities that were scarcely imaginable 15 years ago. The volume of business data worldwide, across all companies, is now doubling every 1.2 years,[4] and more than 90 percent of the world's data was created in the last two years.[5]

Updating the Safe Harbor to reflect these changes is timely. EU-U.S. negotiations must continue – on an expedited timetable and with the vocal support of Member State governments—and a new Safe Harbor must be agreed quickly, ideally well before January 31, 2016. European data protection authorities have already made clear that "[i]f by the end of January 2016, no appropriate solution is found with the U.S. authorities . . . EU data protection authorities are committed to take all necessary and appropriate actions, which may include coordinated enforcement actions."[6]

---

[4] Corry, Will. "BIG Data / The Volume Of Business Data Worldwide, Across All Companies, Doubles Every 1.2 Years, According To Estimates." The Marketing Blog 2012. *available at* http://www.themarketingblog.co.uk/2012/10/big-data-the-volume-of-business-data-worldwide-across-all-companies-doubles-every-1-2-years-according-to-estimates/

[5] IBM, "What Is Big Data"; *available at* http://www-01.ibm.com/software/data/bigdata/what-is-big-data.html

[6] *See* Statement of the Article 29 Working Party (October 16, 2015), available at http://www.cnil.fr/fileadmin/documents/Communications/20151016_wp29_statement_on_schrems_judgement.pdf

Even if there is quick consensus on a new agreement to replace the Safe Harbor, American (and European) companies will need a longer standstill period in which to adapt their operations to the new legal realities. A longer standstill period is essential to preserving the expectation of software and technology providers, companies that rely on these services, and consumers on both sides of the Atlantic.

U.S. and EU negotiators have indicated that they have made significant progress toward a new agreement to replace the Safe Harbor. We encourage them to push forward aggressively with this dialogue, and to agree and announce a new agreement within the next 90 days if possible, with the encouragement of Congress wherever necessary at both the EU and Member State levels.

Looking Ahead

A new agreement to replace the Safe Harbor is a vital and essential step. But it is not the complete solution to the larger issue of privacy protections in the digital age. We urge Congress, and the United States Government more broadly, to look to the longer term.

The European Court of Justice's ruling set a standard of "essential equivalence" between the protections over data in Europe and the United States. What "essential equivalence" means is going to require careful consideration and analysis. One potential place to start is with a comparison of the European Union's and United States' rules and practices in relation to surveillance and law enforcement access to data.

Of course, the United States already has many laws in place that protect against the concerns over "mass and undifferentiated" surveillance raised by the European Court. And the United States has also recently made important reforms to its surveillance laws and processes, including through Executive Orders and the USA FREEDOM Act. These reforms are not well understood in Europe. We urge the United States Government to actively communicate these reforms.

At the same time, we also urge the U.S. Government to listen carefully to Europe's concerns about the extent and the limitations of U.S. law, including in relation to its limited applicability to non-U.S. persons.[7] It may well be that further reform of U.S. law is appropriate to address at least some EU concerns. This change can come through vehicles like the Judicial Redress Act, which BSA strongly supports and which speaks directly to one of the points raised by the European Court. This and similar reforms will help reassure Europeans that their rights will be respected when their data is transferred to the United States. Equally important, and independent of the Safe Harbor controversy, these changes will also reassure customers of American companies around the world.

It is also clear that there are concerns on the European Union side in relation to the transparency of what happens to data collected in the European Union when it is exported to the United States under the Safe Harbor. Significant changes in this space have been made in the past two years. U.S. companies fought for, and won, the ability to provide increased transparency around data requests to all consumers around the world. The U.S. government also has worked to increase transparency around data requests.[8] Creative, and multilateral, approaches will be needed to reach compromise here.

Ultimately, however, "essential equivalence" will be a dynamic concept that will change as European and U.S. laws and practices evolve. Companies cannot, and should not, be expected to update their compliance mechanisms every few years, each time the "essential equivalence" equation shifts. The Safe Harbor lasted nearly 15 years. To achieve that sort of stability, we will need to arrive at a

---

[7] Some of the perceived limitations of the USA FREEDOM Act's reforms have been discussed in a recent study by the European Parliament Directorate General for Internal Policies, "A Comparison between US and EU Data Protection Legislation for Law Enforcement," September 2015; *available online at* http://www.europarl.europa.eu/RegData/etudes/STUD/2015/536459/IPOL_STU(2015)536459_EN.pdf

[8] *See* ODNI Releases Transparency Implementation Plan (describing plans for new efforts as well as US intelligence community efforts to increase transparency in recent years) (Oct. 27, 2015), *available online at* http://www.dni.gov/index.php/newsroom/press-releases/210-press-releases-2015/1275-odni-releases-transparency-implementation-plan.

meeting of the minds between the United States and Europe that will allow for a more enduring solution for data transfers, capable of standing the test of time.

Helpfully there are already several good ideas on the table. For example, a number of commentators have suggested and supported the idea of a new trans-Atlantic—or potentially even broader – agreement that ensures that public authorities in the United States and the European Union can ensure access to data when necessary (wherever that data is held), but in a way that ensures that those demands respect the domestic law of the individual's home country.

The United States and Europe are not as far apart in terms of privacy principles and practices as some might think. Just as privacy is a fundamental human right in Europe, the U.S. Constitution's 4th Amendment enshrines protection from government intrusion, and has done so since 1791. And many American companies already meet European-level data protection standards as a result of their global business operations. Congressional support in communicating this common ground to European leaders is essential to achieving a durable solution.

Where there are gaps that span the Atlantic, whether perceived or actual, we can close these, through a combination of dialogue, domestic legal reform, and international commitments. Congress will be a key part of enabling this to happen.

Thank you again Chairman Burgess, and Ranking Member Schakowsky, Chairman Walden and Ranking Member Eshoo, and members of both Subcommittees for providing this opportunity to share BSA's views on this important matter. I look forward to answering any questions you might have.

Mr. BURGESS. The chair thanks the gentlelady.

Dr. Meltzer, you are recognized 5 minutes for an opening statement, please.

STATEMENT OF JOSHUA MELTZER

Mr. MELTZER. Chairman Burgess, Chairman Walden, Ranking Member Schakowsky, and Ranking Member Eshoo, honorable members of both committees, thank you for this opportunity to share my views with you on the Safe Harbor decision and the impacts for transatlantic data flows.

Transatlantic data flows underpin and enable a significant amount of trade and investment where this concerns personal data of people in Europe and it is subject, therefore, to European privacy laws. The Safe Harbor framework has allowed personal data to be transferred from the E.U. to the U.S., but as a result of a recent decision of the European Court of Justice, the ability to do this has been called into serious question.

I will briefly outline the link now between data flows and transatlantic trade and investment and discuss the potential implications of this European Court of Justice decision.

As has been noted already, the U.S.-E.U. economic relationship is the most significant in the world. In 2014 alone transatlantic trade was worth over $1 trillion. And would you also not forget the importance of the investment relationship with stock of investment in both jurisdictions is over $4 trillion.

Data flows between the U.S. and the E.U. are also the largest globally, 55 percent larger than data flows between the U.S. and Asia alone. These data flows underpin and enable a significant amount of this bilateral economic relationship. Just to give you a couple of examples, businesses use internet platforms to reach customers in Europe. Internet access and the free flow of data supports global value chains, and data flows are essential when U.S. companies with subsidiaries in Europe manage production schedule and human rights and H.R. data.

The global nature of the internet is also creating new opportunities for small and medium-sized enterprises to engage in international trade. For example, 95 percent of those SMEs in the U.S. who use eBay to sell goods and services to customers do so in more than four countries overseas. This compares with less than 5 percent of such businesses when they are exporting off-line. And this is obviously important as SMEs are the main drivers of job growth in the United States, accounting for 63 percent of net new private sector jobs since 2002.

Unfortunately, there is only limited quantitative data on the impact of the internet in cross-border data flows on international trade. If we focus on services that can be delivered online, in 2012 U.S. exported over 380 billion of such services, and over 140 billion of that went to the E.U.

So E.U. privacy laws require entities that are collecting personal data to comply with privacy principles. And when transferring this personal data outside of the E.U., this can only be done under specific conditions. One of these is a finding from the European Commission that the receiving country provides an adequate level of privacy protection, which essentially requires that they have pri-

vacy laws equivalent to the E.U. There are other forms, models, contracts, and binding corporate rules, though these are not well utilized.

The U.S. Safe Harbor framework has allowed for the transfer of personal data from the E.U. to the U.S., despite differences in approaches to privacy protection. In the recent Schrems decision, the European Court of Justice has effectively invalidated this mechanism for transferring personal data from the E.U. to the U.S.

Now, in terms of its immediate impact of this decision, the European data privacy actors have said that they will wait until the end of January 2016 before enforcing Schrems. Since 2014, there has been an effort to renegotiate Safe Harbor, and certainly one solution here would be for the newly renegotiated Safe Harbor agreement to address all the concerns that the European Court of Justice has outlined with the current Safe Harbor framework. However, until we know the outcome of these negotiations and, importantly, whether they are acceptable to the European Court of Justice, there will remain considerable legal uncertainty as to how transfers of personal data from the E.U. to the U.S. can continue.

Failure to find a way for companies to transfer personal data to the U.S. can have significant economic repercussions, and these costs are likely to fall most heavily on small and medium-sized enterprises who lack the resources to navigate the complex legal issues and to manage the risk. In addition, some of the other mechanisms available for the transfer personal data to the U.S. such as binding corporate rules are often not available to small and medium-sized enterprises who do not have a corporate presence in the E.U.

I appreciate the opportunity to offer my views on this important issue and look forward to your questions.

[The prepared statement of Mr. Meltzer follows:]

Subcommittee on Commerce, Manufacturing, and Trade and Subcommittee on Communications and Technology, United States House of Representatives

Hearing on "Examining the EU Safe Harbor Decision and Impacts for Transatlantic Data Flows"

November 3, 2015

Dr. Joshua P. Meltzer
Senior Fellow in the Global Economy and Development program at the Brookings Institution
Adjunct Professor at the Johns Hopkins University School for Advanced International Studies

Introduction

Chairman Burgess, Chairman Walden, Ranking Member Schakowsky and Ranking Member Eshoo, honorable members of both Committees, thank you for this opportunity to share my views with you on the EU Safe Harbor Decision and the impacts for transatlantic data flows.

Summary

- The U.S.-EU economic relationship is the largest in the world, consisting of trade flows valued at over $1 trillion annually and stocks of investment in each economy close to $4 trillion.
- High levels of Internet penetration, trade and investment underpins and is also enabled by data flows between the U.S. and the EU. For instance, in 2012 U.S. exports to the EU of up to $140 billion in value were delivered online.
- Data flows between the U.S. and the EU have led to a large variety of business models, forms of international trade and investment. Businesses in the U.S. use the Internet and data flows to innovate, engage in R&D with European counterparts and to connect to global supply chains. Access to the cloud requires data to move across borders. U.S. businesses also transfer data amongst subsidiaries located across the EU.

- Small and medium-sized enterprises are taking advantage of the Internet and the ability to move data between the U.S. and the EU to engage in international trade. They are using Internet platforms such as eBay to reach consumers and to export.
- The most significant potential barrier to transatlantic data flows is the EU Privacy Directive, which prevents the transfer of personal data outside of the EU to countries that do not have an adequate level of privacy protection—interpreted in the EU as meaning privacy protection that is essentially equivalent to the EU approach.
- Since 2000, the U.S.-EU Safe Harbor Framework has legalized the transfer of personal data from the EU to the U.S., despite differences in the U.S. and EU approaches to protecting personal information.
- The decision of the European Court (ECJ) of Justice in *Schrems* invalidates the European Commission's finding under the Safe Harbor Framework that U.S. privacy protection is adequate.
- Failure to update the Safe Harbor Framework and to respond fully to the concerns of the ECJ about how EU personal data is protected in the U.S. could lead to prohibitions on transferring personal data to the U.S. The impact of such an outcome on transatlantic trade and investment would be significant.

The transatlantic trade and investment relationship

U.S.-EU trade and investment

The U.S. and the EU economies represent over 50 percent of global GDP, 25 percent of global exports and over 30 percent of global imports. The U.S.-EU economic relationship is the most significant in the world. In 2014, total goods trade with the EU was worth approximately $700 billion. In 2014, U.S. exports of services to the EU were worth over $219 billion and imports were approximately $169 billion; leading to total transatlantic trade in 2014 of $1.09 trillion. This compares with total trade with Canada and China of $741 billion and $646 billion respectively.

The transatlantic investment relationship is also the world's largest. The majority of U.S. foreign direct investment is in Europe and this is also true of European investment in the U.S. The total stock of investment that the U.S. and Europe have invested in each other is worth around $4 trillion.

United States and European investment in each other's markets are important drivers of transatlantic trade. Sixty-one percent of U.S. imports from the EU and 33 percent of EU imports from the U.S. consist of intra firm trade, making the sale of goods and services through foreign affiliates in each country key drivers of transatlantic trade. This compares with intra firm trade as a share of U.S. imports from the Pacific Rim (37.2 percent), and South/Central America (37 percent).[i]

The size of transatlantic data flows

The ability to access, accumulate and transfer data across borders is a function of the globalization of the Internet. Data flows between the U.S. and the EU are the largest globally; approximately 55 percent larger than data flows between the U.S. and Asia and 40 percent larger than data flows between the U.S. and Latin America.[ii]

The size of transatlantic data flows reflects Internet penetration in the U.S. and the EU—which is around 85 percent in the U.S. and 90 percent in the EU—and the importance of data as underpinning and often enabling the bilateral economic relationship.

The importance of cross-border data flows for U.S. and EU trade and investment

There are multiple ways that the free flow of data between the U.S. and Europe generates international trade and investment:[iii]

- When a business in Europe uses the Internet to reach customers in the U.S. to sell products online. Internet commerce in the U.S. grew from $13.63 billion in 2011 to $42.13 billion in 2013 and is expected to reach $133 billion in sales by 2018.[iv] As online marketplaces in the U.S. and the EU mature, consumers will increasingly use the Internet to purchase goods and services from each other's markets, thereby growing transatlantic trade.
- Transatlantic data flows underpin business to business transactions, such as when a U.S. business receives financial advice from Barclays in London. This is a financial service that is delivered online and is itself a trade in services. In addition, using the Internet to access such cutting-edge business services can increase the productivity and competitiveness of

businesses, strengthening their ability to compete in overseas markets, further stimulating international trade. According to an OECD study, a 1 percent increase in the importation of business services is associated with a 0.3 percent higher export share.[v]

- Internet access and the free flow of data supports global value chains. This includes so-called trade in tasks[vi]—the ability of geographically diverse businesses to contribute a task or service as part of supply chains that span the Atlantic.
- The free flow of data between the U.S. and Europe is needed for intra-company purposes and is thereby an important enabler of transatlantic investment. For instance, GE in Atlanta relies on the free flow of data to manage production schedules, HR data and communicate internally with its subsidiaries throughout Europe.
- Investment in data centers that provide access to the cloud in the U.S. and Europe relies on cross-border data flows. For instance, Amazon's data centers in Ireland require regular communication with its U.S.-based data centers to update or duplicate data for security purposes. Cross-border data flows are also necessary to reduce latency, such as when Google caches data on servers located closer to EU residents.
- Internet access and the free flow of data provides businesses and entrepreneurs with information on new markets, opportunities for collaboration and research that can support economic activity and lead to international trade between the U.S. and the EU and globally.

Transatlantic data flows also create opportunities for the U.S. and the EU to expand trade and investment with the developing world. As Internet access expands globally, much of the developing world will access the Internet on mobile devices. And by 2018, 54 percent of these devices will be "smart," up from 21 percent in 2013.[vii] Combining these trends with a growing

middle class in Asia in particular–which is expected to double by 2020 – highlights the potential growth of online international commerce. In fact, globally, people who have made at least one online purchase increased from 38 percent in 2011 to 40.4 percent in 2013, and by 2017 over 45 percent of the world are expected to be engaging in online commerce.[viii] The free flow of data globally will be required to ensure these opportunities are full realized.

The Internet is helping SMEs engage in international trade

Small and medium-sized enterprises (SMEs) are key drivers of U.S. growth and employment. SMEs are the main drivers of job growth in the U.S., accounting for 63 percent of net new private sector jobs since 2002.[ix] Over 80 percent of SME job growth is in the services sector.

Yet, SMEs are underrepresented in international trade. The top 1 percent of large firms in the U.S. account for 90 percent of U.S. trade, but only 15 percent of employment.

The global nature of the Internet is creating new opportunities for SMEs to engage in international trade.[x] For example, 95 percent of SMEs in the U.S. using eBay to sell goods and services export to customers in more than 4 continents—compared with less than 5 percent of U.S. business that export offline. And 74 percent of these SMEs are still exporting after 3 years, compared with 15 percent of offline exporters. [xi]

Calculating the value of digital trade

There is only limited data on the importance of the Internet and cross-border data flows for digital trade. One reason is that public trade data does not distinguish between whether goods and services are delivered offline or online. The impact of the Internet on digital trade is also a

function of the digitization of economies broadly, which has made separating out the impact of the Internet on trade (and GDP) a complex task.

Notwithstanding this limitation, some economic modelling has been done that seeks to quantify the relationship between Internet access, economic growth and trade. A World Bank study found that a 10 percent increase in broadband penetration resulted in a 1.38 percent increase in growth in developing countries and a 1.21 percent increase in growth in developed countries.[xii] In terms of the impact of the Internet on trade, one study concludes that a 10 percent increase in Internet access leads to a 0.2 percent increase in exports.[xiii] Other studies using more recent data find even stronger impacts of Internet use on trade.[xiv]

In terms of U.S.-EU trade and investment that is enabled by data flows, by focusing on services that could be delivered online, I calculated that in 2012, U.S. exports of such digitally deliverable services exports globally were $384 billion, and over $140 billion went to the EU.[xv] Services are also traded online through foreign affiliates in each other's markets. In 2011, U.S. foreign affiliates in Europe delivered $213 billion worth of digitally deliverable services and European businesses in the U.S. provided $215 billion worth of such services.[xvi]

The digitization of the U.S. and EU economies means that the Internet is also affecting trade through its impact on productivity, which in turn increases the competitiveness of these businesses domestically and globally.[xvii] For instance, use of the Internet to collect data and analyze it can improve firm productivity by making supply chains more efficient, improving distribution and transport schedules. Indeed, much of the strong productivity growth in the U.S. in the mid-1990s through to the mid-2000s has been attributed to strong investment in

linformation & Communications Technology.[xviii] A recent study of EU firms also found that engaging in e-commerce increases labor productivity—and that e-commerce had accounted for 17 percent of EU labor productivity growth between 2003 and 2010.[xix] A 2014 U.S. International Trade Commission (ITC) report found that the productivity gains from the Internet have increased U.S. real GDP by 3.4-3.5 percent.[xx]

The EU Privacy Directive

Privacy protection is not a new issue. In the 19th century Samuel Warren and Louis Brandeis, concerned about the potential for media to intrude on personal lives, wrote about a "right to be left alone."[xxi] Protecting privacy became increasingly important post-WWII as governments' increasing use of personal data combined with new computing power to process the data. This led to various government reviews of privacy protection and in 1980 the OECD produced *Guidelines on the Protection of Privacy and Transborder Flows of Personal Data*—reflecting an OECD consensus on how member countries should handle and protect personal data.[xxii]

Since these 1980 OECD guidelines, the rise of global Internet access and use has exponentially increased the amount of data that is being or can be combined and processed to create individual profiles. This data is also increasingly valuable and in some cases the value from the collection of this data is the basis on which "free" services such as email and social networking are provided. The global nature of the Internet also means that this data can be quickly and easily transferred to third parties in other jurisdictions. This has raised new challenges for how personal data is used, disclosed, monetized and protected. It has also brought to the fore the

need to find a way to achieve privacy protection while avoiding increasing barriers to cross-border data flows, which can undermine the Internet's economic and trade potential.

Governments are taking different approaches to regulating personal data collected by private enterprise.

The EU Data Protection Directive (DPD) adopted in 1995 governs personal data protection in the EU. As a "Directive," implementation of the DPD is left to EU member states. And in practice, member states vary widely in their enforcement of the DPD. The European Commission is seeking to update the DPD in the form of a Regulation.[xxiii]

The DPD defines personal data as "any information relating to an identified or identifiable natural person", and defines an identifiable person as "one who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more specific factors specific to his physical, physiological, mental, economic, cultural or social identity."[xxiv]

Under the DPD, anyone that processes personal data must comply with five principles. These principles require that personal data is:[xxv]

- Processed fairly and lawfully
- Collected for specific, explicit and legitimate purpose and not further processed in a way incompatible with those purposes
- Adequate, relevant and not excessive in relation to the purposes for which they are collected
- Accurate and where necessary, kept up-to-date

- Kept in a form that permits identification of the data subject for no longer than is necessary for the purpose for which the data were collected

The DPD allows for processing personal data only under specific circumstances. The main ones are where: the data subject has unambiguously given his/her consent; processing is necessary for the performance of a contract to which the data subject is a party, for compliance with a legal obligation to which the controller is subject, to protect the vital interests of the data subject, or it is in the public interest. Processing is also allowed for the purposes of the legitimate interests pursued by the controller, except where such interests are overridden by the fundamental rights and freedoms of the data subject.[xxvi]

For a category of personal data the DPD considers sensitive, such as on racial or ethnic origins, then processing is restricted to situations such as where there is explicit consent, for obligations in the field of employment, or to protect the vital interests of the data subject.

Transferring personal data from the EU to third countries

In the case where the processor is outside of the EU, the transfer of personal data from the EU can only take place under specific conditions.

Adequacy finding

An important mechanism for transferring personal data outside of the EU is for a country to receive a finding from the European Commission that the receiving country provides an adequate level of privacy protection.[xxvii]

So far, outside of Europe and British territories in Europe, only four countries (Argentina, Uruguay, Israel, New Zealand) have been recognized as providing adequate levels of data protection, and Canada and Australia have been recognized as adequate for the purposes of transferring passenger name records. While in determining adequacy the DPD allows for consideration of alternatives to top-down legislated approaches to privacy regulation such as industry self-regulation, all of these countries were found to have adequate privacy protection based on specific economy-wide laws. For instance, Argentina was assessed as providing an adequate level of data protection based on its constitution and other legislation.[xxviii] This was also true for Uruguay.

Model Contracts and Binding Corporate Rules

Personal data can also be transferred to a third country under so-called derogations, the main ones being consent of the data subject, when the transfer is necessary for the performance of a contract between the data subject and the controller, or it is necessary on important public interest grounds.[xxix]

BCRs and contracts are not used much due to the time and expense of getting them approved. Contracts have also been unwieldy for multinational companies, as they must be designed to deal with all possible data transfers, and therefore are unable to respond to issues that might arise without being amended.

In many cases the controller will not have a contract with a data subject. For instance, collecting and processing personal data from Internet use (i.e., "monitoring"), would not create a contractual relationship.

Even where a contract existed, the data transfer must be "necessary" for the performance of the contract. This would include transferring financial and personal information to complete an online transaction but would not include other data incidental to the transaction.

Derogations under the DPD

The DPD also allows for cross-border transfers pursuant to a contract that guarantees the same protection of the personal data as under the DPD. A global conglomerate can transfer data amongst its units where it has implemented binding corporate rules (BCRs) that also ensure data protection consistent with the DPD.

Under the DPD, in order for consent to be effective to authorize cross-border data transfers it must be "specific and informed." This means that merely using an online service that leads to the collection of personal data will not constitute consent. Instead, action such as ticking a box may be required.

The ability to transfer data outside the EU pursuant to a legitimate interest is heavily circumscribed. First, the data must not be frequent or massive so this derogation could not be used to justify an online business that relies on regular data collection. Where businesses seek to use this derogation for more limited data transfers they have to demonstrate that they have put in place appropriate safeguards to protect the data, document the assessment and the appropriate safeguards, and inform the EU supervisory authority of the transfer of data.

The U.S.-EU Safe Harbor framework

The U.S.-EU Safe Harbor framework was developed to respond to a 1999 Opinion from the Article 29 Working Party[xxx] that U.S. privacy protection did not providing adequate protection in all cases for personal data transferred from the EU.[xxxi]

On 26 July 2000, the European Commission recognized the Safe Harbor Privacy Principles and Frequently Asked Questions issued by the Department of Commerce as providing adequate protection for the purposes of personal data transfers from the EU.[xxxii] This Decision allows for the transfer of personal information from the EU to companies in the U.S. that have signed up to the Safe Harbor principles.

The Safe Harbor framework consists of seven principles that largely reflect the key elements of the EU Data Protection Directive. The mains ones are commitments to: give European data subjects notice that a U.S. entity is processing their data; to limit onward transfers of data to countries that also subscribe to the Safe Harbor principles or are the subject of an adequacy finding; to take reasonable steps to protect personal data from loss or misuse; to process

personal data only for the purposes for which the organization intends to use it; to give European data subjects access to their personal information and the ability to correct, amend or delete inaccurate information; and a commitment to enforce the principles and give European data subjects access to affordable enforcement mechanisms.

Under the Safe Harbor framework, U.S. organizations can either join a self-regulatory privacy program that adheres to the Safe Harbor principles or self-certify (most common) to the Department of Commerce that they are complying with these principles. Additionally, U.S. companies must identify in their publically available privacy policy that they adhere to and comply with the Safe Harbor principles. Approximately 4,500 companies are certified under the Safe Harbor framework.

The Safe Harbor framework covers Internet companies and industries including information and computers services, pharmaceuticals, tourism, health and credit card services. Financial services and telecommunications are not subject to Federal Trade Commission Article 5 oversight (see below) and are therefore outside the scope of the Safe Harbor framework. Most of the companies use Safe Harbor to export services to the EU. Subsidiaries of EU firms located in the U.S., such as Nokia and Bayer, also use Safe Harbor to transfer data from the EU.[xxxiii]

Safe Harbor oversight and enforcement

Under the Safe Harbor framework the U.S. Department of Commerce reviews every Safe Harbor self-certification and annual recertification submission it receives from companies. The Department of Commerce also maintains a list of companies on its website that comply with the Safe Harbor Principles.

The FTC enforces the Safe Harbor framework against those companies that self-certify as being in compliance. The FTC can enforce breaches of the Safe Harbor agreement under Article 5 of the Federal Trade Commission Act preventing unfair or deceptive acts. According to the FTC, misrepresenting why information is being collected from consumers or how the information will be used constitutes a deceptive practice. Moreover, under Safe Harbor companies need to certify that they will collect data in accordance with the Safe Harbor principles and the FTC considers that failure to do this would be a misrepresentation and a deceptive practice.

The FTC acts on referrals from EU data protection authorities, third party private dispute resolution providers and on its own.

Safe Harbor framework negotiations

Since 2014 the U.S. and the EU have been renegotiating the Safe Harbor framework. These negotiations started following the Edward Snowden leaks and revelations about NSA bulk surveillance and use of data collected by private U.S. companies that were certified under the Safe Harbor framework. As a result, much of the focus of the European Commission has been addressing the loss of confidence within the EU of the privacy of personal data transferred to the U.S. For example, following the Snowden leaks the Bremen Data Protection Authority requested that companies transferring personal data to the U.S. inform the DPA on how access by the NSA is prevented.[xxxiv]

There is also concern in the EU with U.S. dominance of the I.T. sector. For instance, Google accounts for over 90 percent of Internet searches in Europe. Social networking is dominated by

Facebook and U.S. companies such as Microsoft and Amazon are key players globally when it comes to cloud computing.

As part of the Safe Harbor framework negotiations, the European Commission provided a list of 13 recommendations it wished to have addressed.[xxxv] My understanding is that very good progress has been made on all these recommendations, the most difficult discussions being over how to give effect to recommendations 12, and particularly 13, which requires that the Safe Harbor national security exception is "used only to an extent that is strictly necessary."

The *Schrems* Decision

The case of *Schrems v. Data Protection Commissioner*[xxxvi] before the European Court of Justice (ECJ) addressed whether the Irish Data Protection Authority (DPA) was bound by the European Commission's finding that the U.S., under the Safe Harbor framework, provides an adequate level of protection of persona data. The Irish DPA had found that the Commissions' adequacy decision under the Safe Harbor framework prevented further investigation into whether the use by Facebook of personal data is consistent with the EU Privacy Directive.

The key findings in *Schrems* are:

- The Safe Harbor framework fails to provide an adequate level of protection of personal information for the following reasons:
    - U.S. public authorities are not subject to the Safe Harbor framework
    - U.S. authorities have accessed EU personal data beyond what is strictly necessary and proportionate to the protection of national security

  - There is no administrative or judicial means of redress that allows EU citizens to access their personal data and to have it rectified or erased if needed.
  - The trumping of national security demands when in conflict with the protection of privacy restricts the ability of DPAs to determine compatibility of data transfers with the Safe Harbor framework.
- As a result, the European Commission finding under the Safe Harbor framework that the U.S. provides an adequate level of protection of EU personal information is invalid.
- An adequacy finding by the Commission does not reduce the power of national Data Protection Authorities to determine whether transfers of personal data to the U.S. comply with EU Data Privacy Directive.
- Only the ECJ can declare whether a Commission decisions in invalid.

The Implications of the *Schrems* decision

Following the *Schrems* decision, the Article 29 Working Party—made up of representatives of EU DPAs—stated that it would wait until the end of January 2016 before enforcing *Schrems*.[xxxvii] In the meantime, the Working Party noted that concluding the Safe Harbor negotiations could be part of the solution. Certainly, the European Commission is hoping that the Safe Harbor negotiations can address the concerns laid out by the ECJ.[xxxviii] To achieve this would require passage by the Senate of the Judicial Redress Act.[xxxix] Whether a new Safe Harbor framework satisfies the ECJ will ultimately need to be tested again before that court.

The *Schrems* decision also calls into question the legality of BCRs and contracts for transferring personal data from the EU to the U.S. This is because ECJ concerns about the level of privacy

protection in the U.S. and, in particular, the access of national authorities to personal data for national security purposes would appear to be relevant to all data transfer mechanisms. In this regard, post-*Schrems* German DPAs have called into question the ability to use standards contract and BCRs to transfer personal data to the U.S. and have said that they will not currently issue new authorizations to transfer persona data to the U.S. on the basis of BCRs or model contracts.

Companies can rely on the so-called derogations outlined above, including consent. As outlined, these are limited in scope and therefore are only partial options for companies needing to transfer personal data.

The net result then is considerable legal uncertainty about how to transfer personal data from the EU to the U.S.

The outcome will be particularly costly for SMEs. This is due to the legal and risk management that companies must now undertake—costs that will fall most heavily on smaller companies. In addition, to the extent that BCRs and contracts are still used, these mechanisms are less useful for SMEs. For instance, BCRs apply to conglomerates that have a presence in the EU, which is often not the case for SMEs that are providing online services from the U.S. using Internet platforms.

Conclusion

I appreciate the opportunity to offer my views on this important issue.

---

[i] Daniel S Hamilton and Joseph P. Quinlan, "The Transatlantic Economy 2014", Volume 1/2014

[ii] This figure is based on data over submarine cables. This figure does not necessarily only capture the end-uses of the data, as data often transits though the U.S. and Europe. For instance, data from Latin America can transit the U.S. on its way to Europe and data from Africa can transit through Europe on its way to the U.S.

[iii] Joshua P. Meltzer, "The Importance of the Internet and Transatlantic Data Flows for U.S. and EU Trade and Investment", Brookings Working Paper 79, October 2014

[iv] Statista Dossier, Global internet usage 2014, p. 47

[v] Frederic Gonzales, J. Bradford Jensen, Yunhee Kim and Hildegunn Kyvik Nordas, "Globalisation of Services and Jobs", in Policy Priorities for International Trade and Jobs (OECD 2012), p. 186

[vi] Gene M. Grossman and Estaben Rossi-Hansberg, "Trading Tasks: A simple Theory of Offshoring", 98:5 American Eco Review (2008), p. 1978

[vii] Cisco Visual Networking Index: Global Mobile Data Traffic Forecast Update, 2013-2018, p. 3

[viii] Statista Dossier, Global internet usage 2014, p. 41

[ix] SBA Advocacy 2014

[x] U.S. International Trade Commission, "Digital Trade in the U.S. and Global Economies, Part 1", Investigation No., 332-531, July 2013, p 3-2

[xi] eBay (2015), 2015 US Small Business Global Growth Report

[xii] Qiang & Rossotto (2009), "Economic Impacts of Broadband in The World Bank (2009)

[xiii] Caroline L. Freund and Diana Weinhold (2004) The effect of the Internet on international trade *Journal of International Economics* 62, 171

[xiv] Huub Meijers (2014), "Does the Internet generate economic growth, international trade, or both?" Int. Econ Policy, 11:162

[xv] Joshua P. Meltzer, "The Importance of the Internet and Transatlantic Data Flows for U.S. and EU Trade and Investment", Brookings Working Paper 79, October 2014

[xvi] Joshua P. Meltzer, "The Importance of the Internet and Transatlantic Data Flows for U.S. and EU Trade and Investment", Brookings Working Paper 79, October 2014

[xvii] Bernard, Jensen & Redding (May 2007),Firms in International Trade *Center for Economic Studies, Bureau of Census* (CES 07-14, p. 5

[xviii] Grossman, G.M., Helpman, E., (1991) Innovation and Growth in the Global Economy MIT Press, Cambridge; Baily, M.N., (2002), The new economy: post mortem or second wind? Distinguished lecture on economics in Government. *Journal of Economic Perspectives* 16 (2), 3-22

[xix] Martin Falk & Eva Hagsten (2015) "E-Commerce Trends and Impacts Across Europe, UNCTAD Discussion Paper No. 220, March 2015, UNCTAD/OSG/DP/2015/2, March 2015

[xx] United States International Trade Commission (August 2014), Digital Trade in the U.S. and Global Economies *Part 2 Pub. 4485 Investigation No. 332-540*, 71

[xxi] Samuel D. Warren and Louis D. Brandeis, "The Right to Privacy" in *Harvard Law Review* Vol. IV, No. 6 (15 December 1890)

[xxii] OECD (2013) The evolving privacy landscape: 30 years after the OECD Privacy Guidelines (2011) in The OECD Privacy Framework, OECD 2013, p. 69

[xxiii] European Commission, Proposal for a Regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation), 2012/0011 (COD), Brussels, 25.1.2012. The proposed Regulation includes a Communication from the Commission and a proposed Directive on rules for data processes by authorities for prosecuting criminal offenses. This paper focuses on the Regulation only.

[xxiv] DPD Artilce 2

[xxv] DPD Article 6

[xxvi] DPD Article 7

[xxvii] DOD Article 25

[xxviii] European Commission Decision pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequate protection of personal data in Argentina, C(2003)1731 final, Brussels, 30/06/2003
[xxix] DPD Article 26
[xxx] Advisory working party established under the DPD comprising representatives from Member State data protection authorities and from the European Commission
[xxxi] Working Party on the Protection of Individuals with Regard to the Processing of Personal Data, *Opinion 1/99 Concerning the Level of Data Protection in the United States and the Ongoing Discussion Between the European Commission and the United States Government*, at 4, DG MARKT Doc. 5092/98/WP 15 (Jan, 26, 1999)
[xxxii] Commission Decision 520/2000/EC of 26 July 2000
[xxxiii] Communication from the Commission to the European Parliament and the Council on the functions of the Safe harbor from the Perspective of EU Citizens and Companies Established in the EU / COM/2013/0847 final
[xxxiv] Communication from the Commission to the European Parliament and the Council on the functions of the Safe harbor from the Perspective of EU Citizens and Companies Established in the EU / COM/2013/0847 final
[xxxv] Communication from the Commission to the European Parliament and the Council on the functions of the Safe harbor from the Perspective of EU Citizens and Companies Established in the EU / COM/2013/0847 final
[xxxvi] Maximillian Schrems v. Data Protection Commissioner, European Court of Justice, Case C-362/13, 6 October 2015
[xxxvii] Statement of the Article 29 Working Party, Brussels, 16 October 2016
[xxxviii] Commissioner Jourova's remarks on Safe Harbor EU Court of Justice judgement before the committee on Civil Liberties, Justice and Home Affairs, 26 October 2015
[xxxix] H.R. 1428 – Judicial Redress Act of 2105

Mr. BURGESS. The chair thanks the gentleman.
Mr. Rotenberg, you are recognized for 5 minutes, please.

STATEMENT OF MARC ROTENBERG

Mr. ROTENBERG. Thank you, Mr. Chairman, Ranking Member Schakowsky, Chairman Walden, members of the committee. I appreciate the opportunity to testify today. My name is Marc Rotenberg. I am President of EPIC. I have also taught information privacy law at Georgetown for the past 25 years and study closely the developments of the European Union privacy system.

I need to explain that the Safe Harbor framework from the outset raised concerns among experts, consumer organizations, and privacy officials, many of whom looked at the framework and saw a familiar set of principles but were concerned about the enforcement of those principles. Over the last several years, there have been repeated calls on both sides of the Atlantic to update and strengthen the Safe Harbor framework.

In our comments to the Federal Trade Commission, we routinely ask the agency to incorporate strong privacy principles to give meaning to the Safe Harbor framework, but the agency was reluctant to do so. And so to us and others, the judgment of the European Court of Justice did not come as a surprise. The problems with Safe Harbor were familiar.

But I should explain also this approach to data protection in Europe is familiar in the United States. The European regulators are trying to protect a consumer interest, which is data protection set out in a Charter of Fundamental Rights and attempting to hold foreign companies to the same standards that they would hold domestic companies. We do the same thing in the U.S. with product safety, consumer products, automobiles. Emissions standards, for example, must be equally enforced against foreign auto suppliers, as they are against U.S. firms, because U.S. firms should not have to carry a cost that foreign firms would not. This is essential to understanding the notion of essential equivalence in the judgment of the European Court of Justice.

But another key point to make, which I set out in the testimony on pages 10 and 11, is the language in the Charter of Fundamental Rights. This is the European bill of rights, and they have set out both privacy and data protection as cornerstone rights within their legal system, one protecting the right to privacy and the other explicitly saying that everyone has the right to the protection of personal data. Such data must be processed fairly and such compliance must be ensured by an independent authority.

Now, I know it would be tempting in the context of the current discussion to imagine that a Safe Harbor 2.0 could address the challenge that the European Court of Justice has set out, but my sense is that that approach will not be adequate because part of what the European Court of Justice has identified is also the concern shared by U.S. consumer groups, privacy experts, and others, that the U.S. has not updated its privacy law.

The data not only on European citizens but also on U.S. citizens lacks adequate protection, and that is why in my testimony today I am strongly recommending that you consider long-overdue updates to domestic privacy law, that you not simply see this as a

trade issue. I propose, for example, four specific steps I believe Congress could take that over the long term would solve not only the Safe Harbor problem but would be good for U.S. consumers and for U.S. business.

Specifically, I think the Consumer Privacy Bill of Rights, which the President has proposed and reflects many privacy bills that have gone through this committee as a good starting point. I think updates to the U.S. Privacy Act would make a lot of sense. I know they are already under consideration by Congress. I think the creation of an independent data protection agency in the U.S. is long overdue and could help address concerns on both sides of the Atlantic. And finally, I think we do need an international framework to ensure transborder data flows not only between the E.U. and the U.S. but among all of our trading partners around the world because we are today in a global economy.

Now, I know you may think this is just the view of perhaps privacy people or consumer groups, but I would like to share with you the views that have recently been expressed by leaders of the internet industry. It was Microsoft President Brad Smith who, after the decision of the European Court of Justice, said "privacy is a fundamental human right." It is Apple's CEO Tim Cook who said just 2 weeks ago on NPR "privacy is a fundamental human right." These are the exact same words of the European Court of Justice. This is the view of U.S. consumer groups. I believe on both sides of the Atlantic there is consensus for the view that privacy is a fundamental right.

Thank you.

[The prepared statement of Mr. Rotenberg follows:]

epic.org | ELECTRONIC PRIVACY INFORMATION CENTER

Testimony and Statement for the Record of

Marc Rotenberg
President, EPIC
Adjunct Professor, Georgetown Law

Hearing on

"Examining the EU Safe Harbor Decision and Impacts for Transatlantic Data Flows"

Joint Hearing Before the

United States House of Representatives Energy & Commerce Subcommittees on Commerce, Manufacturing, and Trade and Communications and Technology

November 3, 2015
2123 Rayburn House Office Building
Washington, DC

Testimony Summary

Safe Harbor was an industry-developed self-regulatory trade strategy that simply did not work. Consumer groups and scholars long criticized the Safe Harbor framework, noting that almost a decade passed before the Federal Trade Commission brought an enforcement action against a US company. The decision of the European Court of Justice to strike down the Safe Harbor was not a surprise: transatlantic data transfers without legal protections were never safe.

The Court ruling reflects (1) the weakness of Safe Harbor regime, (2) developments in EU law, and (3) lack of progress on the US side to update domestic privacy law safeguards. The Court's decision reflects the recognition that both privacy (Article 7) and data protection (Article 8) are fundamental rights. The ruling also makes clear that independent national privacy agencies will have the authority to enforce these rights. Enforcement actions are already underway.

But this is not simply a trade issue. The decision of the European Court is also a reminder that US law needs to be updated. American consumers today confront skyrocketing identity theft, data breaches, and financial fraud. All of the polls point to broad-based support, within the United States, for updating privacy safeguards.

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

The United States should not update its privacy law because of a judgment of the European Court. The United States should update its privacy law because it is long overdue, because it is widely supported, and because the ongoing failure to modernize our privacy law is imposing an enormous cost on American consumers.

There is today a growing consensus on both sides of the Atlantic, supported by consumer groups and business leaders, to recognize that privacy is a fundamental human right. Congress should take this opportunity to carry "the American tort" forward into the Information age. This is not simply a matter of trade policy. It is a matter of fundamental rights.

Chairman Burgess, Chairman Waldman, and members of the House Subcommittees, thank you for the opportunity to testify today regarding EU Safe Harbor decision. My name is Marc Rotenberg, and I am President of the Electronic Privacy Information Center ("EPIC"). EPIC is an independent, non-profit research organization focused on emerging privacy and civil liberties issues. We work closely with a distinguished advisory board, with leading experts in law, technology, and public policy.[1] In 2006, EPIC in conjunction with Privacy International, a London-based human rights organization and several hundred privacy experts and NGOs around the world, published the most extensive survey of international privacy law ever produced.[2]

I have also taught Information Privacy Law at Georgetown Law since 1990 and am the coauthor of a forthcoming casebook on privacy law.[3] Much of my scholarly work over the last two decades has been on comparative approaches to privacy protection. I have written extensively on the development of the EU privacy law and also made recommendation on how the US and Europe could move forward to address shared concerns about the protection of privacy.[4]

---

[1] EPIC Advisory Board, https://epic.org/epic/advisory_board.html

[2] EPIC and Privacy International, PRIVACY AND HUMAN RIGHTS: AN INTERNATIONAL SURVEY OF PRIVACY LAWS AND DEVELOPMENTS (EPIC 2006) (The report is over 1,100 pages and contains almost 6,000 footnotes).

[3] ANITA L. ALLEN & MARC ROTENBERG, PRIVACY LAW AND SOCIETY (WEST 2016). *SEE ALSO*, MARC ROTENBERG, JULIA HORWITZ, & JERAMIE SCOTT, EDS. PRIVACY IN THE MODERN AGE: THE SEARCH FOR SOLUTIONS (THE NEW PRESS 2015).

[4] Marc Rotenberg, "Digital Privacy, in US and Europe," N.Y. Times, Oct. 13, 2015; Marc Rotenberg, "On International Privacy: A Path Forward for the US and Europe," *Harvard International Review* (Spring 2014); Marc Rotenberg & David Jacobs, "Updating the Law of Information Privacy: The New Framework of the European Union," *Harvard Journal of Law and Public Policy* (Spring 2013); Marc Rotenberg, "Better Privacy Laws: Priority for America and Germany," N.Y. Times, Sept. 3, 2013

I. Safe Harbor was Never an Effective Basis for EU-US Data Flows.

The Safe Harbor Framework is an industry-developed self-regulatory approach to privacy protection that simply does not work.[5] Coordinated by the Department of Commerce, the Safe Harbor program allows US companies to self-certify privacy policies in lieu of complying with legal requirements for the processing of data of Europeans. The Safe Harbor arrangement developed in response to the European Union Data Directive, a comprehensive legal framework that established essential privacy safeguards for consumers across the European Union.[6] The Federal Trade Commission has been tasked with overseeing Safe Harbor compliance, but only "sanctions" companies by proscribing them from future misrepresentations when they make false representations.

Weaknesses of Safe Harbor Were Known at the Start

Consumer groups and scholars have long criticized the Safe Harbor Framework, noting that almost a decade passed before the Federal Trade Commission ("FTC") brought an enforcement action against a US company with respect to the Safe Harbor.[7] Furthermore, three studies of the Safe Harbor Framework, conducted in 2001, 2004, and 2008, found numerous deficiencies, with the most recent study finding that "the growing

---

[5] U.S. Dep't of Commerce, Safe Harbor Privacy Principles, http://export.gov/safeharbor/eu/eg_main_018475.asp (last updated Jan. 30, 2009).

[6] Directive 95/46/EC of the European Parliament and of the Council of Oct. 24, 1995 on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data, 1995 O.J. (L 281) 31, *available at* http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31995L0046:EN:HTML.

[7] Anita Ramasastry, *EU-US Safe Harbor Does Not Protect US Companies with Unsafe Privacy Practices*, FINDLAW (Nov. 17, 2009), http://writ.news.findlaw.com/ramasastry/20091117.html. See also TACD, Safe Harbor Proposal and International Convention on Privacy Protection (1999) http://test.tacd.org/wp-content/uploads/2013/09/TACD-ECOM-08-99-Safe-Harbor-Proposal-and-International-Convention-on-Privacy-Protection.pdf; TACD, Safe Harbor, 1999 http://test.tacd.org/wp-content/uploads/2013/09/TACD-ECOM-18-00-Safe-Harbor.pdf

number of false claims made by organisations regarding the Safe Harbor represent a new and significant privacy risk to consumers."[8] In 2010, a German state Data Protection and Privacy Commissioner demanded termination of the Safe Harbor agreement, citing low levels of enforcement by the United States.[9] In 2013, the European Commission outlined thirteen changes to strengthen the Safe Harbor protections.[10] The suggested modifications included changes to Safe Harbor's transparency, redress procedures, enforcement procedures, and the extent to which companies allow US law enforcement to access their data.[11]

These Safe Harbor framework problems were widely known at the time of adoption. Consequently, the European Court of Justice's decision to strike down the Safe Harbor arrangement was the culmination of what many experts had warned about all along: transatlantic data flows under the framework were never safe.[12]

---

[8] World Privacy Forum, The US Department of Commerce and International Privacy Activities: Indifference and Neglect, 18 (Nov. 22, 2010), *available at* http://www.worldprivacyforum.org/wp-content/uploads/2009/12/USDepartmentofCommerceReportfs.pdf. *See also* Chris Connolly, Galexia, The US Safe Harbor – Fact or Fiction? (Dec. 2, 2008), *available at* http://www.galexia.com/public/research/assets/safe_harbor_fact_or_fiction_2008/safe_harbor_fact_or_fiction.pdf.

[9] *Id.* at 19.

[10] Communication from the Commission to the European Parliament and the Council— Rebuilding Trust in EU-US Data Flows, COM (2013) 846 (Nov. 26, 2013), available at http://ec.europa.eu/justice/data-protection/files/com_2013_846_ en.pdf; Communication from the Commission to the European Parliament and the Council on the Functioning of the Safe Harbour from the Perspective of EU Citizens and Companies Established in the EU, COM (2013) 847 (Nov. 26, 2013), available at http://ec.europa.eu/justice/data-protection/files/com_ 2013_847_en.pdf.

[11] *Id.*

[12] See generally, Max Schrems v Irish Data Protection Commissioner (Safe Harbor), EPIC (2015) https://epic.org/privacy/intl/schrems/default.html.

The Federal Trade Commission Failed to Pursue Meaningful Enforcement

The FTC is charged with enforcing the US-EU Safe Harbor Framework against US companies that fail to abide by the framework. To date, the FTC has not meaningfully exercised its enforcement powers against US companies that violate the Safe Harbor framework. EPIC has previously urged the FTC to take more aggressive action in Safe Harbor settlements. In 2014, EPIC submitted comments to the FTC after the agency published settlement agreements with 12 companies that misrepresented Safe Harbor compliance. Each of the companies had self-certified to the Safe Harbor Framework, but according to the FTC investigation, failed to renew self-certification while continuing to represent to consumers that they were current members of the Safe Harbor Framework. The FTC's settlement agreements prohibited the companies from making those representations and required them to provide annual reports about their compliance with the agreements, but did not impose any other penalty.

EPIC recommended that the FTC revise the proposed orders to, among other things, require the companies to comply with the Consumer Privacy Bills of Rights. The Consumer Privacy Bill of Rights is a comprehensive framework of seven substantive privacy protections for consumers that would ensure that consumers' personal data is protected throughout the data lifecycle. EPIC explained that by requiring companies to comply with the Consumer Privacy Bill of Rights, the FTC would put in place a baseline set of privacy standards that are widely recognized around the world and necessary to protect the interests of consumers.

Consequences of Inadequate Data Protection in the United States Implicate the Interests of US Consumers and US Businesses

The ongoing collection of personal information in the United States without sufficient privacy safeguards has led to staggering increases in identity theft, security breaches, and financial fraud. These privacy problems have skyrocketed since 2000, but one only needs to look at this year of disastrous data breaches to confirm the magnitude of the problem. This summer a number of retailers, including CVS and Walgreens, lost their customers data through a breach of a common third-party vendor that managed the photo service sites for each retailer. The data breach compromised customer credit card information, names, phone numbers, email addresses, usernames, and passwords.[13] CareFirst BlueCross BlueShield was hit by a data breach that compromised the personal information of over 1 million users. Healthcare insurers Anthem and Premera Blue Cross also suffered major data breaches this year. Overall, these healthcare insurers have lost the data on more than 90 million Americans.[14] Experian, the largest American consumer credit bureau, suffered a breach that compromised the Social Security Numbers of 15 million people. The sensitive information of 21.5 million people was compromised with the data theft from the Office of Personnel Management.[15] The data breach included the loss of Social Security Numbers as well as security clearance applications.

---

[13] Taryn Luna, *CVS Confirms Data Breach at Photo Site This Summer*, Boston Globe (Sept. 11, 2015), https://www.bostonglobe.com/business/2015/09/11/cvs-confirms-data-breach-photo-site-this-summer/xc7mG3YFVgkKLYBQHfrIwI/story.html.

[14] Bryan Krebs, *Carefirst Blue Cross Breach Hits 1.1M*, Krebs on Security Blog (May15, 2015, 9:03 AM), http://krebsonsecurity.com/2015/05/carefirst-blue-cross-breach-hits-1-1m/.

[15] Jim Sciutto, *OPM Government Data Breach Impacted 21.5 Million*, CNN (July 10, 2015), http://www.cnn.com/2015/07/09/politics/office-of-personnel-management-data-breach-20-million/.

These data breaches only represent a subset of the breaches in 2015 and continue a rising trend in data theft—data theft that often leads to identity theft. It is no wonder that identity theft continues to be the top consumer complaint to the Federal Trade Commission and has been for a decade and a half.[16] The rise in data breaches in US companies and identity theft since the implementation of the Safe Harbor has diminished US and EU citizen confidence that their data will remain private and secure. A PEW research poll last fall showed little confidence that the US government or commercial entities would keep data secure.[17] No serious person today believes that the United States has adequate protections in place for personal data.

A "Safe Harbor 2.0" merely repackages the previous framework that the European Court of Justice struck down, and it would not adequately safeguard personal data US companies routinely fail to protect. To encourage transatlantic data flows, Congress must modernize and enforce US privacy law.

II. The Schrems Decision is Far-reaching and the Consequences Could Be Severe if the US Fails to Act

The European Court of Justice struck down Safe Harbor because EU personal data transferred to the United States does not receive the same legal protection in the

[16] Press Release, FTC, Identity Theft Tops FTC's Consumer Complaint Categories Again in 2014 (Feb. 27, 2015), https://www.ftc.gov/news-events/press-releases/2015/02/identity-theft-tops-ftcs-consumer-complaint-categories-again-2014.

[17] Mary Madden and Lee Rainie, *Americans' Attitudes About Privacy, Security and Surveillance*, Pew Research Center (May 20, 2015), http://www.pewinternet.org/2015/05/20/americans-attitudes-about-privacy-security-and-surveillance/.

United States as it does in Europe. Specifically, according to the European standard, the level of protection should be "adequate"[18] and "essentially equivalent."[19]

EU Regulatory Approach for Data Protection is Similar to US Regulatory Approach for Drugs, Foods, Consumer Products, and Cars – Consumers in Domestic Markets are Protected by Meaningful Safeguards

This is a very familiar idea in many US regulatory domains. We do not permit the import of drugs, foods, consumer products, or cars that are not safe for American consumers. It would not be fair to our companies to expect them to comply with our regulatory requirements while allowing non-US firms to ignore the same legal obligations. The same applies to European companies in Europe. It is not fair to expect them to comply with European privacy and data protection laws if the American companies do not have to comply with the same rules. Data transfers to the US are not safe for non-US individuals because the lack of adequate privacy safeguards.[20]

Essentially, the Safe Harbor regime created a legal ground for US companies to circumvent European data protection standards while European companies are bound by those obligations. This has resulted in lower level of protection for Europeans when their data is transferred to the US. The level of privacy protection in the US is lower for Europeans from two perspectives. First, US privacy protections are not as stringent as

---

[18] Article 25(6) of Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data (OJ 1995 L 281, p. 31), as amended by Regulation (EC) No 1882/2003 of the European Parliament and of the Council of 29 September 2003 (OJ 2003 L 284, p. 1) ('Directive 95/46'). See also Marc Rotenberg, Letter to the Editor, The New York Times (October 13, 2015). http://www.nytimes.com/2015/10/13/opinion/digital-privacy-in-the-us-and-europe.html?_r=0

[19] Paragraph 73 of C-362/14, Maximillian Schrems v Data Protection Commissioner, 2015.

[20] Douwe Korff, EU-US Umbrella Data Protection Agreement : Detailed analysis, FREE Group (October 14, 2015). http://free-group.eu/2015/10/14/eu-us-umbrella-data-protection-agreement-detailed-analysis-by-douwe-korff/

Europeans privacy protections. Second, EU citizens do not enjoy the same Privacy Act protections that Americans do. The Privacy Act, as adopted in 1974, defines an "individual" entitled to protection under the Act as a citizen of the United States or an alien lawfully admitted for permanent residence.[21] In recognizing the fact that the US routinely collects data on EU citizens, Congress is considering updating the Privacy Act to extend protections to EU citizens.[22]

The European Court of Justice's holdings were driven in part by the National Security Agency's mass surveillance programs and the failure to establish meaningful regulation of Internet companies, almost all based in the United States. The judgment of the Court reflects also the incorporation of Article 7 and Article 8 of the Charter of Fundamental Rights in EU law. These provisions state

Article 7
Respect for private and family life

> Everyone has the right to respect for his or her private and family life, home and communications.

Article 8
Protection of personal data

1. Everyone has the right to the protection of personal data concerning him or her.
2. Such data must be processed fairly for specified purposes and on the basis of the consent of the person concerned or some other legitimate basis laid down by law. Everyone has the right of access to data which has been collected concerning him or her, and the right to have it rectified.

---

[21] 5 U.S.C. § 552a(a)(2). *See generally, The Privacy Act 1974*, EPIC (2015), https://epic.org/privacy/1974act/.
[22] EPIC's letter to the U.S. House of Representatives Committee on the Judiciary on H.R. 1428, the Judicial Redress Act of 2015 (September 16, 2015). https://epic.org/foia/umbrellaagreement/EPIC-Statement-to-HJC-on-HR1428.pdf

3. Compliance with these rules shall be subject to control by an independent authority.

The Court ruling reflects (1) the weakness of Safe Harbor regime, (2) developments in EU law and (3) lack of progress on US side to develop meaningful and comprehensive privacy safeguards.

The Court also highlighted the enforcement power of the national data protection officials of EU Member States. This means that although they are not entitled to declare an adequacy decision of the European Commission – such as Safe Harbor – invalid, they can and should enforce privacy and data protection rights. This type of enforcement capability[23] is not a new power provided by the Court decision, but it is certainly strengthened and has become more visible[24] after the judgment. This development also reflects the ongoing negotiations about the General Data Protection Reform in Europe.[25] The European Court of Justice's holdings are far-reaching and of global significance. Following the Safe Harbor decision, Israel and Switzerland suspended data flows under Safe Harbor.[26]

Other countries too have taken actions against American firms because we have not yet updated our privacy laws. Jennifer Stoddart, former Privacy Commissioner of

---

[23] Dutch DPA Signs Agreement GPEN Alert System, International Privacy Conference Amsterdam 2015 (October 26, 2015). https://www.privacyconference2015.org/dutch-dpa-signs-agreement-gpen-alert-system/

[24] European Commission Press Release, Speech/15/5916, Commissioner Jourová's remarks on Safe Harbour EU Court of Justice judgment before the Committee on Civil Liberties, Justice and Home Affairs (Libe) (October 26, 2015). http://europa.eu/rapid/press-release_SPEECH-15-5916_en.htm

[25] European Commission Factsheet, Reform of the data protection legal framework in the EU (Last update: October 13, 2015). http://ec.europa.eu/justice/data-protection/reform/index_en.htm

[26] No Easy Way Forward for EU-US transfers of personal data, Privacy Laws (October 28, 2015). http://www.privacylaws.com/Int_enews_28_10_15

Canada said "this is the age of big data where personal information is the currency that Canadians and others around the world freely give away."[27] As a result of her continuous investigation and other enforcement actions against Facebook, the company agreed to make changes to better protect users' personal information on the social networking site and comply with Canadian laws. These changes mean that that the privacy of 200 million Facebook users in Canada and around the world will be far better protected.[28]

In Asia, there is growing concern about privacy issues, new, comprehensive privacy laws in Singapore and Malaysia, the amendment of China's consumer protection law to include data privacy principles, and increased financial penalties in South Korea.[29] The Korean Communications watchdog previously fined Google for unauthorized data collection for Street View[30] and the company is now facing business suspension in Korea because of the firm's participation in the Prism program.[31]

---

[27] Meagan Fitzpatrick, Social media websites ignoring privacy laws, watchdog says, CBCNews(May 29, 2012) http://www.cbc.ca/news/politics/social-media-websites-ignoring-privacy-laws-watchdog-says-1.1197586.

[28] Facebook to make privacy changes, CBCNews (August 27, 2009) http://www.cbc.ca/news/technology/facebook-to-make-privacy-changes-1.780164.

[29] Mark Parsons and Peter Colegate, 2015: The Turning Point for Data Privacy Regulation in Asia?, Hogan Lovells Chronicle of Data Protection (February 18, 2015) http://www.hldataprotection.com/2015/02/articles/international-eu-privacy/2015-the-turning-point-for-data-privacy-regulation-in-asia/.

[30] Jack Purcher, Korea's Communication Watchdog Fines Google $198,000, Patently Apple (January 29, 2014) http://www.patentlyapple.com/patently-apple/2014/01/koreas-communication-watchdog-fines-google-198000.html.

[31] Bahk Eun-ji, Google faces business suspension in Korea, The Korea Times (July 2, 2015) http://www.koreatimes.co.kr/www/news/tech/2015/07/133_182052.html.

European Privacy Officials Will Take Enforcement Action

Since the Safe Harbor judgment was issued last month, we can anticipate many privacy cases.[32] Data protection authorities across Europe are preparing enforcement actions.[33] Some of the European privacy officials will go beyond Safe Harbor and look more closely at alternative data transfer strategies, such as Binding Corporate Rules and Model Contract Clauses.[34] According to the Schrems judgment, they have a legal responsibility to safeguard fundamental rights. Therefore, not even the European Commission—the US negotiating party—has the legal authority to prevent these investigations. [35]

Neither consumers nor businesses want to see the disruption of transborder data flows. But the problems of inadequate data protection in the United States can no longer be ignored. US consumers are suffering from skyrocketing problems of identity theft, data breach, and financial fraud. Not surprisingly, European governments are very concerned about what happens to the personal information of their citizens when it is transferred to the United States. A "Safe Harbor 2.0" does not solve this problem. The US will need to do more to reform privacy law to enable transborder dataflows. It is a well-

---

[32] EPIC, European Data Protection Authorities Conclude Data Transfers under Safe Harbor Now Unlawful (October 17, 2015). https://epic.org/2015/10/european-data-protection-autho.html

[33] Press Release, Statement of the Article 29 Working Party (October 16, 2015). http://ec.europa.eu/justice/data-protection/article-29/press-material/press-release/art29_press_material/2015/20151016_wp29_statement_on_schrems_judgement.pdf

[34] Unabhängige Landeszentrum für Datenschutz, Positionspapier des ULD zum Urteil des Gerichtshofs der Europäischen Union vom 6. Oktober 2015, C-362/14 (October 14, 2015). https://www.datenschutzzentrum.de/uploads/internationales/20151014_ULD-Positionspapier-zum-EuGH-Urteil.pdf

[35] Monika Kuschewsky, Schrems (Safe Harbor) Judgment – German Data Protection Authorities Issue Position Paper, Inside Privacy (October 26, 2015). http://www.insideprivacy.com/international/european-union/schrems-safe-harbor-judgment-german-data-protection-authorities-position/

known paradox that promoting the free flow of personal data across national boundaries requires comprehensive privacy protection.[36]

III. To Support Transatlantic Data Flows, Congress Must Modernize US Privacy Law

Never has the need to update the privacy laws of the United States been more urgent. Identity theft, data breaches, and financial fraud are skyrocketing. Americans today worry about retailers who lose their credit card information, intelligence agencies that gather their phone records, and data brokers that sell their family's medical information to strangers. Industry "self-regulation" has failed and opt-out techniques force consumers to check their privacy settings every time a company changes its business model.[37]

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

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

---

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

[37] Coalition Letter to President Obama, On the Second Anniversary of the Consumer Privacy Bill of Rights (February 24, 2014) https://epic.org/privacy/Obama-CPBR.pdf.

progress is the enactment by Congress. Only enforceable privacy protections create meaningful safeguards.

Second, Congress should modernize the Privacy Act, revise the scope of the Act's coverage and clarify the damages provision. There are many changes that need to be made to the law to protect the interests of Americans, particularly after the terrible data breach that compromised 21.5 million employment records, 5 million digitized finger print files, and even the most sensitive SF-86 forms. The Judicial Redress Act does not provide adequate protection to permit data transfers and it does not address the many provisions in the Privacy Act that need to be updated.[38]

The application of the Privacy Act for non-US Persons is the cornerstone of the E.U.-US Umbrella Agreement.[39] But the current proposed changes to the Privacy Act will not solve the problem as the right of judicial redress is far too attenuated. The much better approach would be to simply revise the definition of "individual" to mean "natural person." This would immediately address the concerns that have been raised outside the United States about the scope of coverage of the Act. Further changes to the Privacy Act would be beneficial for US citizens as well.

Third, Congress should create an independent privacy agency, as Congress contemplated in 1974 when it enacted the Privacy Act.[40] EPIC has previously recommended the establishment of a privacy agency to ensure independent enforcement

---

[38] H.R. 1428 114th Congress Judicial Redress Act of 2015

[39] *See generally*, EPIC, EU-US Data Transfer Agreement (2015), https://epic.org/privacy/intl/data-agreement/index.html.

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

of the Privacy Act, develop additional recommendations for privacy protection, and provide permanent leadership within the federal government on this important issue.[41] This independent privacy agency would be charged with enforcing privacy laws. Enforcement should not be assigned to the FTC, as the FTC has missed many opportunities to strengthen US privacy law. The FTC has failed to enforce its own orders when companies have breached settlement agreements.[42] The Commission routinely fails to require companies found to have violated privacy rules to comply with the Consumer Privacy Bill of Rights. The Commission has made no recommendations for legislation following several, in-depth workshops exploring privacy obstacles consumers confront, including Internet of Things and facial recognition. These missed opportunities, coupled with the fact that the FTC infrequently undertakes enforcement actions, make clear that consumers desperately need a new, independent privacy enforcement agency.

Fourth, The final step to address the growing EU-US divide is to ratify the international Privacy Convention 108, the most-well established legal framework for international data flows.[43] The Privacy Convention would establish a global bias to safeguard personal information and enable the continued growth of the Internet economy. In the absence of a formal legal agreement, it is likely that other challenges to self-regulatory frameworks will be brought.

---

[41] *See, e.g.*, Marc Rotenberg, *In Support of a Data Protection Board in the United States*, 8 *Gov't Info. Q.* 79 (1991); *Communications Privacy: Hearing Before the Subcomm. on Courts and Intellectual Prop. of H. Comm. on the Judiciary*, 105th Cong. (1998) (testimony of Marc Rotenberg), available at https://www.epic.org/privacy/internet/rotenberg-testimony-398.html.
[42] EPIC, EPIC v. FTC (Enforcement of the Google Consent Order) (2015), https://epic.org/privacy/ftc/google/consent-order.html.
[43] *See generally*, EPIC, Council of Europe Privacy Convention (2015), https://epic.org/privacy/intl/coeconvention/.

Conclusion

The United States should not update its privacy law because of a judgment of the European Court. The United States should update its privacy law because it is long overdue, because it is widely supported, and because the ongoing failure to modernize our privacy is imposing an enormous cost on American consumers. According to a Pew survey earlier this year, 74% of Americans believe control over personal information is "very important," yet only 9% believe they have such control.[44] In a Pew survey last year, 80% of adults "agree" or "strongly agree" that Americans should be concerned about the government's monitoring of phone calls and internet communications.[45] 64% believe there should be more regulation of advertisers.[46]

Remarkably, the leaders of US Internet companies have also called for stronger privacy protection and have described privacy, much as the European Court did, as a fundamental human right. Microsoft President Brad Smith recently said, "Legal rules that were written at the dawn of the personal computer are no longer adequate for an era with ubiquitous mobile devices connected to the cloud. In both the United States and Europe, we need new laws adapted to a new technological world."[47] Mr. Smith said simply,

---

[44] Mary Madden and Lee Rainie, *Americans' Views About Data Collection and Security*, Pew Research Center (May 20, 2015), http://www.pewinternet.org/2015/05/20/americans-views-about-data-collection-and-security/.

[45] Mary Madden, *Public Perceptions of Privacy and Security in the Post-Snowden Era*, Pew Research Center (Nov. 12, 2014), http://www.pewinternet.org/2014/11/12/public-privacy-perceptions/.

[46] *Id.*

[47] Brad Smith, *The Collapse of the US-EU Safe Harbor: Solving the New Privacy Rubik's Cube*, Microsoft on the Issues Blog (Oct. 20, 2015), http://blogs.microsoft.com/on-the-issues/2015/10/20/the-collapse-of-the-us-eu-safe-harbor-solving-the-new-privacy-rubiks-cube/.

"Privacy is a fundamental human right."[48] Earlier this year, Apple CEO Tim Cook said, "If those of us in positions of responsibility fail to do everything in our power to protect the right of privacy, we risk something far more valuable than money, we risk our way of life."[49] And then just two weeks ago, Mr. Cook told NPR "privacy is a fundamental human right."[50]

In the realm of regulatory policy, we call this "convergence." There is today a growing consensus on both sides of the Atlantic, supported by consumer groups and business leaders, to recognize that privacy is a fundamental human right. I urge the Congress to take this opportunity to carry "the American tort" forward into the Information age.[51] This is not simply a matter of trade policy. It is a matter of fundamental rights.

---

[48] *Id.*

[49] Caroline Moss, *Apple CEO Tim Cook Delivers a Fantastic, Touching Speech About Why Online Privacy Matters*, Business Insider (Feb. 14, 2015), http://www.businessinsider.com/tim-cook-on-online-privacy-2015-2.

[50] NPR, Apple CEO Tim Cook: 'Privacy Is A Fundamental Human Right' (Oct. 1, 2015), http://www.npr.org/sections/alltechconsidered/2015/10/01/445026470/apple-ceo-tim-cook-privacy-is-a-fundamental-human-right.

[51] Following the publication of the famous Brandeis Warren article in 1890, European scholars referred to the privacy claim as "the American tort."

Mr. BURGESS. The chair thanks the gentleman.
Mr. Murphy, you are recognized for 5 minutes, please.

STATEMENT OF JOHN MURPHY

Mr. MURPHY. Mr. Chairman, Ranking Member Schakowsky, distinguished members of the committee, it is an honor to appear before you this morning on behalf of the U.S. Chamber of Commerce, the Nation's largest business association representing companies of every size, sector, and state. And it is representing those companies that I would like to share my comments.

We have spoken this morning about the importance of the international movement of data and how important it is to companies of all kinds. I can speak on behalf of this dynamic and multifaceted array of member companies to confirm that.

Examples of data flows take many forms, including a small exporter operating through an e-commerce portal, a large company with operations in multiple countries managing its human resources, a wind turbine sending data on its performance to the engineers who keep it running, or a transatlantic tourist using a credit card. In short, today's hearing isn't really just about internet companies but about companies. It isn't about the internet economy; it is about the economy.

However, as we have heard, the tremendous benefits of transatlantic data flows are now at risk. The invalidation of the Safe Harbor agreement raises serious questions. I would point out that before its decision, the European Court of Justice did not conduct any formal investigation into U.S. current surveillance oversight. In fact, the decision was based largely on process concerns internal to the European Union.

Even so, more than 4,000 companies have been left asking whether they can continue to transfer personal data from Europe. They are now faced with the tough choice of deciding whether to continue their transatlantic business or face potentially costly enforcement actions.

While companies in the Safe Harbor program continue to guarantee a high level of data protection for the users of their products and services, alternatives cannot be devised overnight. Data privacy systems are complex legally and technically. One alternative suggested by the European Commission, binding corporate rules, can cost over $1 million and take at least 18 months to develop and implement. This is a nonstarter for small businesses.

Or consider a U.S. hotel chain with locations across Europe, each of which works with a host of small businesses that might provide food for their in-house restaurant or janitorial services. All of those relationships involve data flows, and that means there are hundreds of arrangements across hundreds of properties that may need to change at considerable cost.

Another example comes from the auto industry, which uses Safe Harbor to identify vehicle safety issues and for quality and development purposes. However, the industry now faces the challenge of meeting both U.S. and E.U. regulatory requirements, which made diverge. Under U.S. law, auto manufacturers must share a vehicle identification numbers of cars sold globally in the event of a vehicle

service campaign such as a recall. This U.S. obligation may now conflict with E.U. privacy rules.

So what is the outlook? Companies may be faced with a patchwork of 28 different enforcement and compliance regimes in different E.U. member states or more where local governments are involved. There is a serious disconnect between the E.U.'s stated goals of spurring innovation and fostering a startup culture and statements by some European officials about the need for IT independence and calls for data localization.

Further, some in Europe are trying to use legitimate concerns about data protection as an excuse for protectionism, and the uncertainty facing business worsens. This approach has been frequently rebuked by many others in the E.U., but it merits careful scrutiny.

While the business community is committed to working with our European colleagues to ensure a balanced and proportionate system of rules, we must be vigilant. We must ensure that the European Union does not hold the United States to a different standard on national security and law enforcement issues.

Specifically, what should be done? First, we need a new and improved Safe Harbor agreement that reflects current circumstances. The Chamber greatly appreciates the efforts of the Department of Commerce and the FTC to provide clarity and reach an agreement on a revised Safe Harbor. Further, we applaud the House for taking an important first step toward resolving related concerns with the passage of the Judicial Redress Act, and we are encouraging the Senate to act swiftly to give this bill final passage.

The recently announced Umbrella Agreement is also another important step forward allowing data sharing in certain circumstances between law enforcement and national security agencies. Also important are other safeguards instituted in the United States in recent years that provide a level of protection equivalent to or even greater than that found in the European Union and among its member states.

The Chamber appreciates the opportunity to provide these comments to the committee, and we stand ready to assist in any way possible to ensure data flows can continue across the Atlantic.

[The prepared statement of Mr. Murphy follows:]

Statement of the U.S. Chamber of Commerce

ON: The EU Safe Harbor Decision and Impacts for Transatlantic Data Flows

TO: United States House of Representatives
Committee on Energy and Commerce
Subcommittee on Commerce, Manufacturing, and Trade

BY: John Murphy
Senior Vice President for International Policy
U.S. Chamber of Commerce

DATE: November 3, 2015

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.

Chairman Burgess, Chairman Walden, Ranking Member Schakowsky, Ranking Member Eshoo and distinguished members of the committees, my name is John Murphy, and I am Senior Vice President for International Policy at the U.S. Chamber of Commerce (Chamber). I am pleased to testify today on the European Court of Justice (ECJ) Safe Harbor decision and its impact on transatlantic data flows. 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 it is dedicated to promoting, protecting, and defending America's free enterprise system.

Together, the United States and the European Union account for nearly half of global economic output, with each producing approximately $17 trillion in GDP. Total U.S.-EU commerce—including trade in goods and services and sales by foreign affiliates—tops $6 trillion annually and employs 15 million Americans and Europeans.

The U.S.-EU investment relationship is without peer. Companies headquartered in EU Member States had invested more than $1.7 trillion in the United States by the end of 2014 and directly employ more than 3.5 million Americans. Similarly, U.S. firms have invested $2.5 trillion in the EU—a sum representing more than half of all U.S. investment abroad. It's also nearly 40 times as much as U.S. companies have invested in China.

Almost all of this trade and investment is dependent on some form of digital services, whether through direct interactions with customers over the Internet, intra-company human resources management, or a European visitor using a credit card while vacationing in Washington, D.C.

The United States and the EU are global leaders in digital trade, which contributes more than $8 trillion annually to the global economy. The "Internet economy" represented $2.3 trillion or 4.1% of global GDP in 2010 and is expected to reach $4.2 trillion and 5.3% by 2016. One recent study has shown the benefits of a secure, stable, and interoperable Internet reaching as high as $190 trillion by 2030.[1]

These numbers may even underestimate the economic importance of these digital connections to the world economy. Consider, for example, the fact that three-quarters of the value created by digital trade accrues to firms not usually viewed as "Internet companies," such as manufacturers, retailers, and banks. In short, today, there are no Internet companies: There are only companies. And there is no Internet economy: There is only the economy.

Importance of Cross-Border Data Flows

The strength of the U.S.-EU economic relationship relies on the seamless flow of data across borders. While many immediately think of services such as email, in fact cross-border data flows are integral to Chamber members of every size and sector—from small businesses to multinationals, from banking to manufacturing to healthcare. Data is also transferred for

[1] See a recent report by the Atlantic Council and Zurich Insurance finding an optimal "Cyber Shangri-la" would result in substantial global economic gain http://www.atlanticcouncil.org/news/press-releases/atlantic-council-zurich-insurance-report-finds-the-global-benefits-of-cyber-connectivity-expected-to-outweigh-costs-by-160-trillion-through-2030.

purposes well beyond just the personal and commercial, including public health and safety concerns.

For example, medical device manufacturers routinely transfer data across the Atlantic for maintenance and repair purposes. In many cases sophisticated medical equipment cannot be transported to repair facilities, but skilled technicians can provide real-time service on large medical equipment across the Atlantic to facilitate effective patient care. In this case, cross-border data transfer restrictions literally could have life or death consequences for patients.

Data transfers are also used to prevent fraudulent activity, identifying criminals who, after racking up huge debts in one country, are able to start fresh with a clean slate by moving to another jurisdiction. Credit histories that follow individuals across borders also affect 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.

Safe Harbor and the European Court of Justice Decision

However, the overwhelming benefits of transatlantic data flows are now endangered due to the reverberations of the recent ECJ decision on Safe Harbor. The U.S.-EU Safe Harbor agreement was developed to help companies comply with a 1995 EU law that prohibits the transfer of personal data to any country that does not provide "adequate" protections for the use of that data. Only five countries outside Europe[2] are deemed "adequate," with the United States being "adequate" only to the extent that a company is committed to the Safe Harbor obligations—a commitment overseen by the Federal Trade Commission (FTC). It should be noted that the EU's "adequacy" determinations do not follow a set process.

Safe Harbor has served as a valuable tool for companies of all sizes and sectors to assure Europeans that companies are meeting EU data protection standards for a variety of business-to-consumer and business-to-business functions. For example, a U.S.-based education institution may use Safe Harbor to provide online services to remote students across the European Union. Or a Texas-based startup may provide data analytics for a German-headquartered energy company. Or very simply, many multinational companies use Safe Harbor to ensure employees around the world are paid; manage global supply chains; and ensure compliance with certain legal requirements, including SEC reporting.

On October 6, the ECJ ruled that the Safe Harbor agreement is invalid because it does not preclude U.S. authorities from accessing the personal data of Europeans and using it in a way that is "beyond what is strictly necessary and proportionate to the protection of national security." The ECJ also noted the inability of European citizens to seek redress for inaccurate personal information held by the authorities. That said, the decision itself was based largely on process concerns—namely, the EU Commission did not conduct a thorough analysis of U.S. national security standards at the time of the original Safe Harbor agreement and that the agreement attempted to unduly restrict Member State enforcement duties. The decision did not address the actual substantive commercial data protection rules, which are the focus of Safe Harbor.

---

[2] Argentina, Canada, Israel, New Zealand and the United States (for Safe Harbor); see "Commission Decisions on the Adequacy of the Protection of Personal Data in Third Countries," available at http://ec.europa.eu/justice/data-protection/international-transfers/adequacy/index_en.htm.

Impact of the Safe Harbor Decision

The decision had a very real and very immediate impact across the Chamber's entire membership. First, more than 4,400 companies, each of which apply Safe Harbor rules on a routine basis, were faced with immediate uncertainty about whether they could continue transferring personal data from Europe, as absent Safe Harbor the Court indicated such transfers are prohibited. They are now faced with the tough choice of deciding whether to continue their transatlantic business or face the potential for expensive enforcement actions, all while providing the same high level of data protection.

As an initial response to the uncertainty, the EU Commission suggested companies switch to other mechanisms to ensure the protection of personal data, such as binding corporate rules (BCR) or model contract clauses. Both mechanisms have limitations, and in any event the idea fails to take into account the realities of the complex technical systems needed to ensure strong privacy protections.

While companies in the Safe Harbor program continue to ensure a high level of data protection for the users of their products and services, developing compliance mechanisms other than Safe Harbor cannot happen overnight. Data privacy systems are legally and technically intricate and are often developed in connection with security protocols to keep data safe and bad actors away.

One supposedly simple solution that many in the EU Commission and the European Parliament have pointed to—BCRs—can cost more than $1 million and take 18 months to fully implement, from development to approval, and they are limited to governing how personal data is used within a corporation. The process is so complex that only about 70 companies are currently certified.[3] Even if Data Protection Authorities across Europe increased their approval process rate tenfold, such a Herculean effort could not swiftly address the challenge confronting the 4,400 companies left in limbo. Worse, German Data Protection Authorities have announced a temporary halt to approving new BCRs pending clarification of the ECJ's decision.

Another alternative, model contract clauses, might require a reexamination of tens of thousands of transfers. Model contract clauses are neither comprehensive nor flexible: They are largely impractical for when data is received directly from hundreds of customers.

More fundamentally, because the ECJ judgement is based on the right to privacy in the European Charter of Fundamental Rights, it is unclear that *any* of these mechanisms can work so long as the Court's rational for rejecting Safe Harbor stems from its finding that U.S. authorities have excessive and indiscriminate access to personal data held by companies. Further, the implications of such a finding reach far beyond the United States as many—indeed most—countries lack the political and judicial oversight our law enforcement and intelligence services face, and as such transfers of personal data to those countries should be prohibited. In this context, it is critical to note that the ECJ did not conduct any formal investigation in current U.S. surveillance oversight rules.

[3] See "List of companies for which the EU BCR cooperation procedure is closed," available at http://ec.europa.eu/justice/data-protection/international-transfers/binding-corporate-rules/bcr_cooperation/index_en.htm.

Importantly, the decision is felt not just in the United States or with Safe Harbor companies, but in the European Union as well because some services may no longer be offered to European users. Indeed, there may be instances in which U.S.-based companies choose to discontinue using EU-based third-party service vendors, particularly in smaller EU markets. The impact will undoubtedly be felt hardest by small and medium-sized enterprises (SMEs) that cannot afford large legal teams to conduct the thousands of reviews necessary.

Even in cases where a large multinational company seemingly has ample resources, there are often relationships with hundreds of sub-processors, typically SMEs. For example, consider the example of a large U.S.-headquartered hospitality company operating hotels in every EU Member State, often managing multiple properties in each. Each of those hotels in turn works with numerous small companies processing data, covering everything from operating customer rewards programs to in-house restaurant service and food supply. That means there are hundreds of arrangements across hundreds of properties that need to be reviewed and potentially changed. In situations like this, the multinational company may decide it is much easier to perform those services in-house, rather than be exposed to potential risk by continuing to work with those EU-based small businesses.

Another example we have heard from member companies is a large agricultural company that uses a personal expense vouchering system managed by a third-party platform on a global basis. After an initial analysis, company executives realized they might need now to negotiate data protection contracts with that processor for each of the firm's 60 legal entities in Europe. However, in the absence of guidance as to whether even these contracts might meet EU requirements, they have been unable to act.

The auto industry uses Safe Harbor to identify vehicle safety issues and for quality and development purposes. However, the industry now faces issues meeting both U.S. and EU regulatory requirements. Under U.S. law, auto manufacturers must share vehicle identification numbers of cars sold globally in the event of a vehicle service campaign, including recalls. This U.S. obligation, given the invalidation of the self-certification provisions of the Safe Harbor framework, may now conflict with EU privacy rules, creating a conundrum for automakers. This is just one example of the significant impacts that the recent ECJ Ruling will have on automakers' fundamental operations.

U.S. and European Government Responses

The Chamber greatly appreciates the efforts of the Department of Commerce to provide clarity and reach an agreement on a revised Safe Harbor. We recognize that Secretary Pritzker and her colleagues in the FTC have been working very hard to address concerns raised by the ECJ decision. The groundwork to a revised Safe Harbor has already been laid by conversations over the past few years.

Surprisingly, the ECJ decision did not examine recent changes to U.S. oversight of electronic surveillance, which certainly are relevant to the criteria the ECJ believes must be met to be considered "essentially equivalent" to the safeguards that exist in the EU. The Chamber is confident that the recently announced Umbrella Agreement and the swift passage of the Judicial

Redress Act, combined with other safeguards instituted since 2013,[4] provide a level of protection equivalent to or even greater than that found in the European Union and among its Member States.

We are encouraged by recent statements by Secretary Pritzker and EU Commissioner for Justice, Consumers and Gender Equality Věra Jourová indicating that an agreement on a revised Safe Harbor has been reached in principle. The Chamber remains hopeful that these efforts will result in needed guidance within the January 2016 timeline laid down by the European Union. However, the desire to provide clarity has not been universal.

Long-Term Impact

While it is critical that our governments continue to work expeditiously to announce a revised Safe Harbor agreement, we also want to sound a note of caution that even a renewed agreement will not serve as a panacea to all uncertainty for transatlantic business, or indeed all businesses in the European Union.

The ECJ decision affirmed the need for individual Member State Data Protection Authorities to conduct independent investigations into all complaints. Moreover the decision indicated the Commission cannot limit this through findings of "adequacy" in programs such as Safe Harbor. This means that companies may be faced with 28 different enforcement and compliance regimes, and potentially 40 if we include the German state-level data protection authorities.

In fact, Hamburg's Data Protection Officer indicated that the only way to avoid future investigations is to localize data, stating "[a]nyone who wants to remain untouched by the legal and political implications of the judgment, should in the future consider storing personal data only on servers within the European Union." [5]

This uncertainty, coupled with a tendency by some in Europe to use legitimate concerns about data protection as an excuse for protectionist policy, underscores the need to carefully monitor long-term developments in the EU beyond Safe Harbor. For example, a recent resolution by the European Parliament on Safe Harbor specifically called for "greater IT independence.[6]" There is a significant disconnect between the EU's stated goals of spurring innovation and fostering a startup culture and officials' statements about the need for IT independence and calls for localization.

This approach has been frequently rebuked by many in the EU, notably by Andrus Ansip, the EU Commission Vice President in charge of the Digital Single Market, who has pushed back

---

[4] See, e.g., an analysis of recent changes to U.S. national security practices oversight, including, the Privacy and Civil Liberties Oversight Board issued a nearly 200-page report in July 2014 on possible improvements to surveillance safeguards in the United States. Subsequently, the PCLOB found that "the administration has accepted virtually all recommendations in the… report" https://iapp.org/news/a/dont-strike-down-the-safe-harbor-based-on-inaccurate-views-on-u-s-intelligence-law/. See also more on why the U.S. currently is equivalent or greater to the EU, see http://datamatters.sidley.com/wp-content/uploads/2015/10/Memo-re-Section-702-10-25-15-Final.pdf.

[5] http://thehill.com/policy/cybersecurity/258341-germany-to-investigate-google-facebook-data-transfers-to-us.

[6] http://www.europarl.europa.eu/sides/getDoc.do?type=MOTION&reference=B8-2015-1092&language=EN.

against notions that the EU is acting with underlying protectionist intent, explaining that "our doors are open, not closed."

While we are committed to working with our European colleagues in an effort to ensure a balanced and proportionate system of rules, we urge Congress and the United States government to remain vigilant to ensure that the European Union does not hold the United States to a different standard on national security and law enforcement issues, and that it otherwise ensures a level playing field for all actors. And by level playing field, we mean one that serves to boost innovation, rather than tear down or constrain those most widely used products and services.

Conclusion

The United States, the EU and its Member States share common values as strong democracies with an enduring commitment to civil liberties and the rule of law. For this reason, we are befuddled that some in the EU would put such an important economic relationship in jeopardy even as we remain hopeful that pragmatic decision-making and leadership will win the day.

The importance of data flows is too great to allow precipitous changes in policy to undermine them: Recent studies estimate that cutting off data flows between the United States and the EU would cut EU GDP by as much as 1.3%.[7] Given continued slow economic growth in the EU, our closest trading partner, that kind of hit to the EU economy would have significant negative repercussions on this side of the Atlantic as well.

We applaud the House for taking an important first step towards resolving these concerns with the passage of the Judicial Redress Act. We are encouraging the Senate to act swiftly to give this bill final passage.

This week, a group of European Parliamentarians are in town as part of the Transatlantic Leadership Dialogue, presenting our Congress with a perfect opportunity to voice the importance of the Safe Harbor and cross-border data flows, educate them on the oversight Congress exercises over U.S. intelligence and law enforcement agencies, and to ensure they understand the difference between commercial and national security and law enforcement related issues. We encourage you all to seize this opportunity.

Above all, as we have indicated, we urge U.S. and EU officials to move swiftly to put in place a revised Safe Harbor that addresses the concerns that have been raised.

The Chamber greatly appreciates the opportunity to provide these comments to the committee. We stand ready to assist in any way possible to ensure data flows can continue across the Atlantic.

---

[7] The Economic Importance of Getting Data Protection Right; https://www.uschamber.com/sites/default/files/documents/files/020508_EconomicImportance_Final_Revised_lr.pdf

Mr. BURGESS. The chair thanks the gentleman for his testimony, and thank all of you for your being here this morning and sharing your thoughts with us. We are going to move into the question part of the hearing, and I am going to begin by recognizing Mr. Walden 5 minutes for his questions, please.

Mr. WALDEN. I thank the chairman, and I thank all of you for your testimony. It is most enlightening and helpful as we wrestle with this issue ourselves.

Ms. Espinel and Mr. Murphy, do you think the Department of Commerce needs to be doing anything differently to arrive at Safe Harbor framework that will stand up to scrutiny by the European legal system, and if so, what would that be?

Ms. ESPINEL. So I would say, first, I want to thank the Department of Commerce for all the work they have been doing in negotiating the Safe Harbor. And our understanding is that talks are well underway and we are at the moment cautiously optimistic that we will be able—we meaning the United States and the European Union—will be able to find our way to a new Safe Harbor agreement.

And so on that I think the Department of Commerce is doing all that they can. I would continue to urge Congress to encourage the Department of Commerce to focus on that, and also to the extent you are speaking to your European counterparts, to encourage the Europeans to come to a speedy conclusion on a new Safe Harbor agreement.

But I would also say that a new Safe Harbor agreement, while I think it is the immediate short-term step that we need, it will not solve the larger issue. And so I think we need to focus first and foremost at the moment on resolution of the new Safe Harbor agreement, but I think we need to quickly turn to coming up with a longer-term, more sustainable, global solution for data transfers. And that is something that we would like to be working with Congress on and will be working closely with the Department of Commerce, the FTC, as well as the governments of the European Union and the European Commission.

Mr. WALDEN. All right. Mr. Murphy?

Mr. MURPHY. I would agree with those comments. Just briefly, the Department of Commerce has made every effort to get ahead of this problem. In fact, before the European Court of Justice decision had advanced significantly towards reaching a new agreement, obviously further negotiations were required after the ruling came out to reflect those findings. But they have done a good job, and they have done a good job reaching out to the business community to gather their input as well.

Mr. WALDEN. OK. Dr. Meltzer, what impacts will continuing uncertainty around transatlantic data flows have on foreign direct investment both in the United States and the European Union from your perspective?

Mr. MELTZER. Thank you for the question. I think it is important to recognize that the implications of the Schrems decision at the moment are going to be direct on those who are certified under the Safe Harbor framework, but the implications are potentially a lot more significant. We already see in the E.U., for instance, that some of the data protection authorities in Germany have effectively

stated that the other mechanisms that the E.U. has for transferring data—namely, standard model contracts and binding corporate rules themselves—are likely to be available for transferring personal data to the E.U.

So effectively, there is enormous legal uncertainty around the whole process and available options for making this to happen. So one would expect that, for the moment, all forms of foreign investment that essentially are relying on incorporating the transfer of personal data are going to have to be reviewing their processes, and a lot of investment decisions and trade is going to be placed under that sort of higher level of risk and uncertainty for the time being.

Mr. WALDEN. And I noted in some of the testimony, too, it is not just the E.U. anymore. I mean, other countries are looking at this, what the E.U. has concluded, and now they are starting to question whether their own Safe Harbor agreements were correct. And somebody tell me how this is spreading and what we need to be cognizant of going outward. Mr. Rotenberg?

Mr. ROTENBERG. Thank you, Mr. Walden. I do discuss in my prepared statement efforts that actually preceded the judgment of the European Court in Canada, in Japan, in South Korea, and part of the point that I am trying to make today is that this is not simply a matter of trade policy. In other words, where countries have established fundamental rights, they will see a need to protect those rights.

And the second part of the Schrems decision doesn't just invalidate Safe Harbor. It says that each one of the national data protection agencies has the authority to enforce fundamental rights, which means even in agreements between the Department of Commerce and the Commission could be challenged by a member country.

Ms. ESPINEL. But if I could just add briefly——

Mr. WALDEN. Please do.

Ms. ESPINEL [continuing]. There are a number of countries around the world that are looking to put or considering putting trade barriers in place to restrict the movement of data across national borders for a variety of reasons. This is a fight that we have been fighting for at least 5 years now market to market around the world. I think one of the recent inventories of countries that are considering put the number at 18, including significant trading partners such as China but also Russia, Nigeria, and a number of other trading partners.

So while the subject of this hearing is the U.S.-E.U. Safe Harbor, and that is a subject of great concern to us, there is a larger issue here, I think, about setting up a global framework that allows data to move freely around the world beyond just the United States and Europe.

Mr. WALDEN. Thank you. My time is expired.

Mr. BURGESS. The gentleman yields back. The Chair thanks the gentleman for his questions.

The Chair recognizes the gentlelady from Illinois, the ranking member of the Subcommittee on Commerce, Manufacturing, and Trade, 5 minutes for questions, please.

Ms. SCHAKOWSKY. Thank you, Mr. Chairman.

It has been reported that the Department of Commerce and the European Union have agreed, at least in broad strokes, on a replacement for Safe Harbor. And like you, I support passage of a comprehensive privacy bill and a comprehensive data security bill. However, I also hope that the new deal for Safe Harbor can be reached soon and that it will contain significant protections for consumers.

Mr. Rotenberg, in answering the following, please put aside your call for changes to domestic law for a moment. I will ask you that question a bit later. But in your opinion, what should be in the new agreement if there is to be a new agreement to afford consumers stronger privacy protections?

Mr. ROTENBERG. It is a difficult question to answer. There are 13 specific proposals that were presented by the European Commission to the Department of Commerce, and the Department of Commerce and FTC has tried in this negotiation to address the issues that have been raised.

But the reason that it is a difficult question to answer, as other witnesses have pointed out, is that neither the Commerce Department nor the FTC has legal authority over the surveillance activities undertaken by police or intelligence agencies in the United States. And you could say that is kind of a deal-breaker on the European side because it is explicit in the opinion of the Court of Justice that there must be legal authority to restrict that type of mass surveillance.

And I won't go into that debate right now, but the question that you have asked, which is how do you solve the issues that have been identified post-ruling in the Safe Harbor negotiation, I actually don't think there is an answer to. And this even puts aside my recommendation for changes in domestic law. I think that is the reality on the European side as they look at next steps in this process. So in your recommendations for changes in the domestic law, you aren't looking at the issue of government surveillance?

Mr. ROTENBERG. Well, certainly, yes. I mean the Freedom Act was a significant step forward for privacy protection in the United States, but it limited only the surveillance activities directed toward U.S. persons. That is the 215 collection program. The Freedom Act did not address the 702 program, which was collection directed toward non-U.S. persons. And that remains a key concern on the E.U. side. And I don't think that the Department of Commerce can negotiate that in the context of a Safe Harbor 2.0. So at a minimum I think that would have to be done to comply with the judgment of the court.

Ms. SCHAKOWSKY. So there have been various press accounts, and of course, the terms of the new agreement have not been made public, but are there certain provisions that you do consider helpful? For example, we have heard that there will be increased transparency. Is that something that you think they——

Mr. ROTENBERG. Well, it would be good, but to be fair, in the original Safe Harbor proposal, which we were involved with, we actually favored the principles. We said these are familiar principles. They exist both on the U.S. side and on the European side, and they seem like a good basis to promote transborder data flows. We

were not against the principles in the original Safe Harbor, but the problem was the lack of enforcement.

And you see the lack-of-enforcement issue continues even in the Safe Harbor 2.0 because unless Federal Trade Commission or, as I have proposed, an independent data protection agency, has the authority to enforce those principles, it won't have a significant impact on how it is viewed on the European side.

But I agree. I think the steps are in the right direction, but they don't solve the enforcement problem.

Ms. SCHAKOWSKY. In April, Mr. Rush, Congressman Rush and I offered an amendment in the nature of a substitute to the Data Security and Breach Notification Act that would require commercial entities that owned or possessed consumers' personal information to create and implement security procedures to safeguard that data, among other things. Those procedures would have to include processes for identifying, preventing, and correcting security vulnerabilities. Is this important in domestic——

Mr. ROTENBERG. Yes, actually, I think that is a very important proposal. Because there is increasing awareness on both sides of the Atlantic of the need for data breach notification, the Europeans have recently updated their law in part in response to developments that have taken place in U.S. law. And I think your proposal would carry that process forward in a way that is favorable again for consumers and businesses. I don't think this is a process that puts consumers against business. I think we are all on the same page wanting to maintain transborder data flows. So to the extent that these changes help strengthen consumer confidence, I think it is a step in the right direction.

Ms. SCHAKOWSKY. Thank you. I would like to have further conversations with you at another time. Thank you very much. I yield back.

Mr. BURGESS. The chair thanks the gentlelady, and the chair will recognize himself 5 minutes for questions.

Dr. Meltzer, you have indicated in your testimony that cross-border data flows affect small and medium-sized business. Can you give us an idea as to what that effect is?

Mr. MELTZER. So the effect is in multiple ways. I apologize for some generality. As I mentioned in my opening statement, there is unfortunately a paucity of very high data on this issue. EBay, I mentioned, has been particularly helpful in providing data about the way that small businesses export on its platform, and I think it is a good example because it captures a lot of the ways that small businesses are using the internet to access customers globally, and that is certainly the case when it comes to transatlantic trade. And so there is one example where there is a lot of new opportunities for engagement in the global economy by small businesses that really was not possible before that relies on cross-border data flows.

We will have a component of that, which is certainly personal data, which is going to be significantly potentially inhibited by the ruling in the Schrems decision. And as I think has been mentioned before, this is an issue which is transatlantic-specific but is global in its implications.

One of the things I think is worth recognizing is also that there is essentially a global debate going on about the appropriate form of privacy model protection going forward. There is the U.S. version, which is essentially embodying the APEC cross-border privacy principles, and there is the E.U. approach, and both models are being discussed in different form globally. and different countries are looking at different approaches, and which way they go will have a significant impact on how small businesses operate not only on a transatlantic basis but how they use the internet to leverage and engage globally in all countries around the world.

Mr. BURGESS. Well, along those lines then, the benefits that occur to small and medium-sized enterprises, they are not unique to the United States-European Union relationship?

Mr. MELTZER. No, absolutely not. And in many respects the opportunities for small and medium-sized enterprises are as real here as they are in Europe, as they are actually in a range of other countries, including specifically developing countries, which have been be able to engage in international trade in a way that was not possible. So the potential implications of this are much broader than the transatlantic nature, are certainly broader than for the SME sector here in the U.S., but certainly globally.

Mr. BURGESS. Thank you, and I thank you for those answers.

Mr. Murphy, the Chamber of Commerce obviously represents a broad range of interests across the country. Can you give us a sense what you are hearing from your members, how important it is that the United States and European Union reach a new agreement on a new Safe Harbor?

Mr. MURPHY. Well, it is indispensable to U.S.-E.U. economic relationship. It is without peer in the world today. And, as I think several members of the committee have pointed out, bilateral trade is $1 trillion annually, but that doesn't even capture the additional $5 trillion in sales by U.S. affiliates in Europe or European affiliates in the United States. There is no relationship like that. U.S. investment in Europe is 40 times what U.S. companies have invested directly in China. So getting this right matters for all kinds of companies.

I think for small businesses, they are just waking up to it. Dr. Meltzer's comments about eBay and the large number of companies that use that platform as exporters and the uncertainty about what that would mean for them.

But I think that there are potential hidden costs for many small businesses as well. For instance, I gave my example about a hotel chain operating in Europe and the many small businesses which provide services to that hotel. Certainly, many of them have never thought about this. In the absence of a revised Safe Harbor agreement, companies may face an incentive to bring that kind of work in-house, and that could be very damaging for small businesses going forward.

Mr. BURGESS. So what is the current state of risk for your members, and then, further, is that level of risk sustainable for them?

Mr. MURPHY. I think that we are going through a bit of a state of shock here in the wake of the ruling. There was a wide expectation that the ruling might be in some way adverse. I think the full dimensions of it were not fully appreciated in advance. So there is

a circling of the wagons right now to try and work with the authorities to find a solution in the near term.

I do agree with Ms. Espinel, though, that this is an issue that even in the happy event that we are able to achieve in the next weeks or couple of months a new Safe Harbor agreement, this issue is going to require constant attention to get it right on a global level.

Mr. BURGESS. And thank you for your responses.

The chair yields back and recognizes Mr. McNerney 5 minutes for questions, please.

Mr. MCNERNEY. I thank the chair and I thank the witnesses, very interesting hearing this morning.

Mr. Rotenberg, in my mind there is a significant distinction between government surveillance on the one hand and data breach from non-state actors, businesses, or so on on the other hand that are trying to get information that they shouldn't have. Which do you feel is more significant in the Schrems decision?

Mr. ROTENBERG. Well, the Schrems decision looks primarily at a commercial trade framework, which is what Safe Harbor was, and concludes that that trade framework did not meet the adequacy requirement of European law. So in that respect I guess you could say it is commercial. But you see, from the European perspective, because privacy is a fundamental right, the question of who gets access to it in some respects is not as significant. It is the underlying privacy interest. So both will remain important. The European privacy officials will look to whether the personal data that is being collected is used for impermissible reasons either on the commercial side or on the intelligence side.

Mr. MCNERNEY. Have you been keeping up with the exceptional access question here in the United States?

Mr. ROTENBERG. I am not sure if I understand the question.

Mr. MCNERNEY. Well, the FBI and other organizations want to have an encryption key——

Mr. ROTENBERG. Right.

Mr. MCNERNEY [continuing]. That is accessible to them so they can look at data with proper provisions. Do you think that that would hurt our businesses?

Mr. ROTENBERG. Well, I certainly think that would be a mistake. I understand the Bureau's concern. We have had this discussion for many, many years. At the risk, of course, of the so-called key escrow approach to encryption is that you leave systems vulnerable to——

Mr. MCNERNEY. Right.

Mr. ROTENBERG [continuing]. Cyber criminals. In the best of circumstances you can execute your lawful investigation, but we know from experience there are many other scenarios, and those weaknesses will be exploited.

Mr. MCNERNEY. Well, what are some of the differences in between data protection in the U.S. and data protection in Europe?

Mr. ROTENBERG. Well, I actually think there is much more similarity between the two approaches than people commonly think. The European Union privacy law mirrors many of our own privacy laws, our Fair Credit Reporting Act, our Privacy Act. All of these U.S. laws have many of the same principles that the Europeans do.

The difference, I think, is that we have not updated our laws as the Europeans have, so the divide that you are seeing today is really not one about disagreement as to what privacy protection means. It is really divide over the scope of application.

Mr. MCNERNEY. Thank you. One more question for you. Do you have specific recommendations then for data privacy? It sounds like what you are saying is that we really should be more proactive in terms of keeping up——

Mr. ROTENBERG. Yes——

Mr. MCNERNEY [continuing]. With the scope of the problem.

Mr. ROTENBERG. I think we should update our national law. Again, it is obvious there is no benefit to consumers to see the disruption of transborder data flows. Everyone wants to ensure that the data flows continue. But we also know that the weaknesses in U.S. privacy protections will continue even with a new Safe Harbor. So there has to be within the United States an effort to update our privacy law, I believe.

Mr. MCNERNEY. Thank you. Ms. Espinel, will American service members stationed in Europe be able to communicate as easily with their loved ones here in the United States absent Safe Harbor?

Ms. ESPINEL. That is an excellent question, and I think, you know, there are clearly going to be a number of impacts, and I am happy to speak to those. I think we don't know today what the full extent of those impacts will be, but communication between the United States and Europe, I think, is clearly one of the things that could be implicated, among a number of other things as well.

Mr. MCNERNEY. Well, how can U.S. companies ensure that our service members are not cut off from their families?

Ms. ESPINEL. So I would say there are three things that we need to happen. The first is one that we have talked about already today, which is that we need to come to a new resolution for the Safe Harbor. So that is sort of a first immediate step. The United States and Europe need to come together to agree on a new Safe Harbor.

The second thing that we need is we need some appropriate amount of time for U.S. companies to be able to come into compliance with those new regulations. And then, as we have been discussing today, we need to be actively working on what a long-term, sustainable solution is going to be. I think we are all in agreement that while it is enormously important to come to a new agreement on the Safe Harbor as quickly as possible, that will not be our long-term solution and we need to be working together on a long-term, sustainable solution.

Mr. MCNERNEY. So you pivoted back to your opening remarks, then, on the three things that we need to do?

Ms. ESPINEL. I think those are the three things that we need to keep a laser focus on.

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

Mr. BURGESS. The chair thanks the gentleman. The gentleman yields back.

The chair recognizes the gentlelady from Tennessee, Mrs. Blackburn, 5 minutes for questions, please.

Mrs. BLACKBURN. Thank you so much, Mr. Chairman, and thank you all for answering the questions and being right to the point. We appreciate that.

Mr. Meltzer, I wanted to come to you. Your October 2014 working paper on transatlantic data flows, some great stats in there and they really cause you to think when you look at the worth of the digitally exported services and how that does affect our trade. So thank you for that and for making that available.

I want to go back to something Chairman Burgess was beginning to push on a little bit, the short- and long-term consequences as we look at solidifying a Safe Harbor framework. And back to the issue of U.S. businesses, whether they are large or small, and let's talk about between now and January 2016 and what the impact is going to be as you have got that Article 29 Working Party trying to finalize the Safe Harbor agreement. So I would like to hear from you, just let's narrow this focus down and look at these businesses between now and January 2016. We know the volume that is being exported and look at what you think the impact is going to be and then what consequences do you see arising if a new Safe Harbor agreement is unable to be finalized.

Mr. MELTZER. Yes, thank you for that question. So to the first part, assuming that the data protection authorities, all of them, speak to the commitment not to enforce the Schrems decision until the end of January 2016, then we are presumably still in a reasonable status quo environment and data flows should continue, though under a certain amount of increased uncertainty.

Post-January, the question is going to be whether Safe Harbor has been concluded. But as I think the witnesses have said, I think even with conclusion of Safe Harbor, it is still ultimately going to be a question of whether the satisfies the European Court of Justice, and these will most likely have to be ultimately settled again by the European Court of Justice because the data protection authorities have been given the clear authority to investigate complaints regarding adequacy of data flows. So I would imagine a situation even after concluded Safe Harbor 2.0 where you still get data protection authorities looking into whether in fact there is adequacy. So this is certainly going to increase the risk environment.

Stepping back a little bit, I think that there is clearly a significant interest on the U.S. side to make sure that this is resolved. I think this is an equally important interest on the E.U. side to resolve this issue as well. The costs to the E.U. economy are also going to be very significant if they don't manage to resolve this transborder data flow issue. So I think those two dynamics give me some hope that a solution is going to be found, but a number of steps, I think, are going to have to be taken before that is going to be clear.

Mrs. BLACKBURN. OK. Ms. Espinel, do you think they will reach an agreement, and what do you see as the stumbling blocks?

Ms. ESPINEL. We are, as I said, confident, strongly cautiously optimistic that the Department of Commerce and the European Union will be able to come to an agreement. All indications are that the discussions are going well. And as Dr. Meltzer pointed out,

there are very strong interests on both sides of the Atlantic to coming to an agreement.

So, while not wanting to diminish the difficulties inherent in that, we do believe that they will come to an agreement in the short-term, although I feel duty-bound to emphasize that we also believe that the short-term agreement will not be the end of this discussion, that we will need to come up with a long-term solution, both to serve the interests of larger companies but also to serve the interests of the many small and medium-sized businesses that are affected by this and the millions of customers on both sides of the Atlantic that are affected.

Mrs. BLACKBURN. Thank you. I am out of time, but I am going to submit a question for answer dealing with transfer rights, which I think is something that we probably should be having a discussion on also.

So I will yield back.

Mr. BURGESS. The gentlelady yields back. The chair thanks the gentlelady.

The chair recognizes the gentlelady from New York, Ms. Clarke, 5 minutes for questions, please.

Ms. CLARKE. I thank the chairman, Mr. Burgess, and I thank our witnesses for their testimony this morning.

Ms. Espinel, we know that big companies will likely be able to use their legal and technical solutions to get by without Safe Harbor, but what about small businesses? And do small businesses have the resources and expertise necessary to implement alternatives?

Ms. ESPINEL. So that is a fantastic question, and as has been pointed out earlier in this hearing, most of the companies that are affected by the Safe Harbor are small and medium companies. There are two different aspects of this. One way, obviously, to try to deal with this is to build data centers around the world. That is a solution that is out of reach to all but the very largest of companies around the world. It is also a very inefficient way to do remote computing and data analytics. And in fact, it is not only inefficient, it is impossible if information is siloed in different locations. So that is not an option for the smaller companies.

And the difficulties of living in a world where there is a patchwork of regulations is even harder for smaller companies to deal with. It is no picnic for the larger companies to be sure, but I think it is impossible for smaller companies. And I think one of the things that it does is there are enormous efficiencies from remote computing, from cloud computing, from data analytics that benefit big companies, but they also benefit small companies, in some ways even more. As Chairman Walden said, 75 percent of the value-add there is to traditional industries, and there are many small companies across all economic sectors that are affected by this. And putting a shadow over what are still relatively nascent industries, cloud computing and the data analytics at this point, I think it is hard to actually measure what the negative impact of that would be going forward.

Ms. CLARKE. So if you were to advise small companies, given what we know right now in the negotiations, what sort of infra-

structure or construct would you advise these smaller companies to begin looking at?

Ms. ESPINEL. So, as I said, some options are just completely out of the reach of small companies. I think what the small companies need is in line with what we would recommend generally. We all of us need to have a new Safe Harbor agreement in place. We all of us need some appropriate amount of time to come into compliance with those new regulations. And then we all need a long-term solution that is going to work. And that long-term solution, I think, needs to have at least three aspects to it. One, we talked a lot about the importance of privacy. I think it is important that whatever long-term solution there is it provides that a person's personal data will attract the same level of protection as it moves across borders.

We need to have a solution that will allow law enforcement to do the job that it needs to do and protect citizens around the world, and we need to have a solution that will reduce the amount of legal uncertainty that exists right now, not just for big companies but for small companies as well.

Ms. CLARKE. So, Mr. Murphy, given the Safe Harbor ruling's impact on small businesses, are your organizations doing anything to ensure that small businesses have the understanding, expertise, resources necessary to continue their business operations without a Safe Harbor agreement?

Mr. MURPHY. Well, at present, the circumstances don't really provide workable alternatives. As I mentioned in my testimony, the European Commission, in the wake of the ruling by the European Court of Justice, indicated that one valid alternative is to use what is called binding corporate rules. But as Cam Kerry, the former general counsel at the Department of Commerce has pointed out, implementing these can cost $1 million and can take 18 months. This is completely out of the reach of most of our small business members. While larger companies may be able to move in some cases to adopt such an approach, there is really no alternative for the small companies to revise Safe Harbor agreement.

Ms. CLARKE. Have any of you panelists—I only have a few seconds left—given any thought to sort of the nuance that has to be an agreement that would address the concerns of small business in our country?

Mr. ROTENBERG. What we haven't discussed is the role of innovation in the internet economy. And our view is that privacy rules would actually encourage innovation, particularly with small firms. And what I have in mind is to the extent that small and medium enterprises can develop their services in way that minimizes the privacy risk, it also reduces the regulatory burden, because what happens when people look closely at these data protection assessments, they ask what kind of data is being collected? Is the credit card information secure? Do you need the Social Security number? I think small businesses can actually compete in this space by coming up with business practices that are actually modeled practices for privacy protection. That is what I would recommend.

Mr. BURGESS. The gentlelady yields back. The chair thanks the gentlelady.

The chair recognizes the gentleman from Texas, the chairman emeritus, Mr. Barton, 5 minutes for questions, please.

Mr. BARTON. I want to thank both chairmen for this joint hearing, and it is a very important topic.

I am in a little bit of a dilemma. I am the long-term co-chairman of the Congressional House Privacy Caucus, and I am also a pro-business Republican, so if I put my pro-business hat on, I want to renegotiate this Safe Harbor agreement as quickly as possible with as little muss and fuss as possible. But if I put my privacy caucus co-chairman hat on, I think the European Union has highlighted a substantial issue, and that the U.S. privacy laws aren't as strong as they could be and that people like me think they should be.

So I guess my first question to Mr. Rotenberg would be what is the primary difference between the European Union privacy protections for their citizens and the privacy protection currently under law here in the United States?

Mr. ROTENBERG. Well, first of all, Mr. Barton, I actually wanted to thank you for all of your work as a pro-business Republican in support of consumer privacy. I think you help demonstrate that in this country privacy is actually a bipartisan issue, and it is compatible with business.

But I think the point you make is also critical, which is that the Europeans have brought attention to areas of U.S. privacy law where we have more work to do. We have a good framework. Our Privacy Act of '74 is a good law, our Fair Credit Reporting Act of 1970 is a good law, but these are old laws. They have not been updated. We really haven't thought yet about biometric identification, genetic data, facial recognition, secretive profiling of consumers. These are real issues. And the Europeans have spent the last decade trying to understand how to protect privacy while promoting innovation.

So my answer is I think we should continue down the road, which we actually started in the U.S., which is protecting privacy in law, but keep moving forward. I think the European decision provides that opportunity.

Mr. BARTON. Under the current negotiations that are going on between the U.S. and the European Union to come up with a new Safe Harbor agreement, does the U.S. delegation have the authority to make substantive changes in U.S. policy, or are we trying to finesse the substantive disagreement and come up with just a better administrative solution?

Mr. ROTENBERG. I think it will ultimately be for Congress to make the changes in U.S. law that are necessary to provide adequate protection not only for the European customers of U.S. businesses but also for the U.S. customers of U.S. businesses.

Mr. BARTON. Mr. Murphy, do you agree with that?

Mr. MURPHY. Our read of the ruling of the European Court of Justice is that it was fundamentally a federalism issue within Europe having to do with the role of the European Commission on privacy versus the role of the data protection agencies in the 28 member states. And to a significant degree the renegotiation of the Safe Harbor reflects their need to reorganize how they address privacy and the dissatisfaction with how it was handled by the Commission.

That is a complex process. Federalism is always complicated. I don't have to tell a Member of Congress. But the ruling itself was more process-related and about those issues than it was about U.S. privacy protection. After all, there was no comprehensive examination of U.S. privacy law in the context of the European Court of Justice ruling.

Mr. BARTON. Mr. Chairman, it is rare that there is not a silver lining in every issue, and this is an example of where in the short term we want to work with our negotiators to solve this problem because small businesses and large businesses all over the United States need access to the European market and need to be able to transfer data and information seamlessly back and forth. But in the somewhat longer term, perhaps it will give impetus to this committee and the Congress to address some of the fundamental issues and hopefully come up with stronger privacy protections for our citizens.

And with that, Mr. Chairman, I yield back.

Mr. BURGESS. The gentleman yields back. The chair thanks the gentleman.

The chair recognizes the gentlelady from California, Ms. Eshoo, 5 minutes for questions, please.

Ms. ESHOO. Thank you, Mr. Chairman. And I apologize to the witnesses that I had to step out. There is a memorial service for I just think one of the greatest individuals that ever served in the Congress, the late Congressman Don Edwards. So I hope that the questions that I ask haven't already been asked. If they have been, it is because I had to step out.

First of all, Mr. Chairman, I would like to ask for unanimous consent to submit for the record a November 3 letter from the Internet Association to the chairs and the ranking members of C&T and CMT subcommittees.

Mr. BURGESS. Without objection, so ordered.

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

Ms. ESHOO. And I thank you for that.

I mentioned in my opening statement what I think is a major issue in this on the part of the E.U., and that is what type of access the European data and American intelligence agencies, you know, what should be given over because there is a very, very large issue. I mean it is like right under the sheets, and that is that—well, you all know what has taken place relative to the surveillance and what was carried in the mainstream press where American companies, products were stopped from being shipped, things were inserted in those products, repackaged, and sent off. Now, that is, I believe and others believe, really damaging to the brand American product. And the Europeans are deeply suspicious of that.

So, first of all, what I would like to ask you is how would you handle that with the E.U.? Do you believe that there should be an adjustment on the part of our country because this is a big concern of theirs? And if so, how so? So just go quickly so I just get a flavor from each one of you what your thinking is on this issue.

Ms. ESPINEL. So I would just say quickly that is clearly something that the opinion focused on as well. I think we need to—and that is why we have been focusing on we need a short-term solution but we also need a long-term solution because we know that

negotiation of Safe Harbor will not address all of the larger issues, including that one.

USA Freedom Act I think was a good example of our Congress being able to balance privacy and national security, so we would be looking to work with Congress on this issue in the future, and we are confident that that——

Ms. ESHOO. Do you think that the Europeans——

Ms. ESPINEL [continuing]. Balance can be found.

Ms. ESHOO [continuing]. Understand the steps that we took very well? Or do you know of those conversations having taken place so that the knowledge is deeper and broader? I don't think we cured everything, must frankly. We really never do because you have to develop consensus, and these are tough issues.

Ms. ESPINEL. So I think that is a fantastic point, and I think one of the things that we really need is to have a political environment that is cooperative and constructive. And so one of the things that I would respectfully urge Congress to do, when you are talking to your counterparts in the European Union, that I would urge the Administration to do that we can do as well is to help the Europeans understand our privacy system better, including some of the recent improvements like the USA Freedom Act.

I take this opportunity to thank you all for voting for the Judicial Redress Act and hope that the Senate follows your leadership on that.

Ms. ESHOO. Great. Let me just get one more in to you and to others. This weekend, the CEO and cofounder of Virtru authored an op-ed in VentureBeat in which he suggested that encryption and anonymization are ways to adapt to the E.U.'s new data rules. Do you agree? Do you disagree? Do you think it is helpful? Do you think that it will——

Mr. ROTENBERG. This is almost exactly——

Ms. ESHOO [continuing]. Serve our interests?

Mr. ROTENBERG. Yes, this is almost exactly the point I was making to Congresswoman Clarke. I actually think both of those techniques, encryption and anonymization, provide an opportunity for internet-based businesses to minimize their privacy burdens. I think it would be——

Ms. ESHOO. Has anyone taken this on voluntarily that you know of?

Mr. ROTENBERG [continuing]. A very good step forward.

Ms. ESHOO. Any companies to your knowledge taken this on voluntarily?

Ms. ESPINEL. In terms of encryption——

Ms. ESHOO. To adopt these practices——

Ms. ESPINEL. So I would just say that——

Ms. ESHOO [continuing]. Post-Snowden——

Ms. ESPINEL [continuing]. Our companies care deeply about privacy. Many of them have adopted various encryption practices in order to protect their customers' data.

Ms. ESHOO. Thank you to the witnesses. Again, thank you, Mr. Chairman.

Mr. BURGESS. The gentlelady yields back. The chair thanks the gentlelady.

The chair recognizes the gentleman from New Jersey, Mr. Lance, Vice Chairman of the Commerce, Manufacturing, and Trade Subcommittee, 5 minutes for questions.

Mr. LANCE. Thank you, Chairman, and good morning to the distinguished panel. And I commend you, Mr. Chairman and the other chairman, Mr. Walden, for this very important hearing.

This is obviously a challenge based upon the decision, but I think we have the expertise and the bipartisan cooperation, particularly in this committee, to overcome the challenge and to work together to an effective solution. And I guess in the short-term or intermediate term, it is the negotiations now occurring but then moving forward. My estimate would be is that we probably ultimately need legislation. I would like the view of each member of the panel on whether I am correct on that, current negotiations, but then perhaps we will have to have legislation as well, to each member of the distinguished panel.

Ms. ESPINEL. So in terms of having a long-term sustainable——

Mr. LANCE. Yes.

Ms. ESPINEL [continuing]. Global solution, we will need to work with a number of countries on that, including the United States.

I would say I don't want to dismiss the improvements that have been made to our legislation recently in the last couple of years and beyond legislation such as the President's Order number 28 and increase FTC enforcement. I do think we may need to look at other legislative options in the future. And we would obviously like to be working closely with Congress on that. But I think in order to come up with a global framework, we will be needing to work with governments around the world to either update their systems or to have a principle-based approach that is flexible enough that it could work within all of our systems.

Mr. LANCE. Thank you. Dr. Meltzer?

Mr. MELTZER. Yes. I agree that a significant amount of progress has been made here domestically. I mean the issues around surveillance and collecting personal data is one which is obviously important domestically and has been driven by domestic factors rather than what the E.U. wants the U.S. to do. And I think that will continue to be the case.

This discussion with the E.U. tends to be a bit distorted because the European Commission has no authority over national security issues. So what is missing in this debate on the E.U. side is actually the fact that the national security agencies are more or less doing very much what the NSA does and probably with a lot less due process. So we need to remember that this is not necessarily—the U.S. has got a particular balance between national security and privacy, which is working through, and this debate also needs to be, I think, invigorated when we talk about this in the E.U. context as well.

Mr. LANCE. And before answering, Mr. Rotenberg, let me say I share Chairman Emeritus Barton's concerns regarding privacy. And I think it is certainly possible to be a business-centric, relatively conservative Republican and greatly interested in privacy. And then I think it is also possible obviously on the other side, on the Democratic side. So your views as to whether we will need legislation ultimately?

Mr. ROTENBERG. Thank you. I am quite certain you will need legislation. And let me tell you what I think will happen——

Mr. LANCE. Yes, sir.

Mr. ROTENBERG [continuing]. If you don't have legislation.

Mr. LANCE. Yes, sir.

Mr. ROTENBERG. If you only have a revised Safe Harbor 2.0 and you don't address these 702 problems and wait until 2017 when that expires and you don't solve the problem that the FTC actually doesn't have enforcement, I think you will almost immediately see European data protection agencies attack the revised agreement. So to have a meaningful agreement that addresses the concerns that have been set out in the court's opinion, you have to do at least those two things. You have to update 702 and you need enforcement authority for the FTC.

Mr. LANCE. Thank you. Mr. Murphy—and I am certainly interested in you with the Chamber of Commerce because you represent what is best in America and our entrepreneurial spirit.

Mr. MURPHY. Well, thank you. Certainly, it is in the realm of a pro-business conservative to support privacy in businesses as well.

Mr. LANCE. Of course.

Mr. MURPHY. Privacy is indispensable.

Mr. LANCE. Of course. Of course.

Mr. MURPHY. And companies take this very seriously.

I would just add a clarification, though, that with regard to whether or not there should be further privacy legislation in the United States, the ruling of the European Court of Justice does not provide a roadmap for that. It was process-oriented. It had to do with federalism within the European Union. It did not assess in any comprehensive way U.S. privacy laws.

Mr. LANCE. Substantive—yes, it was a procedural matter.

I think this is very helpful, and I am sure we will continue to work with the entire group. And this is an important issue. And, Mr. Chairman, I yield back at 17 seconds.

Mr. BURGESS. The gentleman yields back. The chair thanks the gentleman.

The chair recognizes the gentleman from Vermont, Mr. Welch, 5 minutes for questions, please.

Mr. WELCH. Thank you very much, Mr. Chairman, and thank the witnesses.

Mr. Rotenberg, you mentioned that if we are—the legislation would have to address the 702 problem and provide FTC enforcement, correct?

Mr. ROTENBERG. [Nonverbal response.]

Mr. WELCH. I want to ask you, Mr. Murphy, whether that would be problematic for you to allow the FTC to actually have the enforcement authority and to address the 702 problem.

Mr. MURPHY. I don't think we are in a position to assess that right now, but as a general rule, the business community has felt that the FTC does have extensive abilities to enforce U.S. privacy laws that exist. And we are constantly trying to educate our European colleagues about the misconceptions may have about the U.S. privacy regime. There is——

Mr. WELCH. Well, let me just interrupt a second because this is really pretty critical. You have got, I think, general agreement here

that we definitely want to have this Safe Harbor agreement extended. We want to be able to have this fluid flow of information back and forth really for business reasons. There is a general agreement on privacy. But in order for there to be real enforcement, there has to be some mechanism to take action in the event there is a breach that then gets us sometimes in this committee into a debate about the authority of, in this case, the FTC to act. There are a lot of folks, I think, who are pro-business who would be in favor of proper enforcement as long as it didn't go overboard. So I am just looking for some indication from you as to the openness from your perspective as someone who would be advocating for the business advantages of having that include a proper enforcement by a regulatory agency like the FTC.

Mr. MURPHY. It is something that I think calls for further investigation with our membership.

Mr. WELCH. OK. Ms. Espinel, let me ask you a few questions. Thank you very much, by the way.

Just to recount the amount of business that goes back and forth, I mean, what are the implications for your industry in the event this problem is not solved?

Ms. ESPINEL. So the implications are very significant, and it is not just the nearly 5,000 companies that have used the Safe Harbor. It is the millions of customers that rely on that. But there are all sorts of other implications as well. For example, one of the things that we talk about in the area of cybersecurity is that you need information to follow the sun. You need cyber threat information to be in the hands of experts, wherever they are awake around the world, as quickly as possible. And things like the revocation of the Safe Harbor put that at risk.

Many of the companies that rely on the Safe Harbor using that in part to process payroll so that their employees back at home can be paid on time. Revocation of the Safe Harbor puts that at risk.

I am confident that there are apps being developed in every district represented in this room. If those small companies, those small app developers want to extend into Europe, the revocation of the Safe Harbor puts that at risk.

But more generally, the enormous business efficiency gains by both big companies and small companies from remote computing, from data analytics cannot work unless data can move across borders. So the revocation of the Safe Harbor, one of the big risks there is that it takes all of that efficiency, all the enormous potential gained from that efficiency and puts them at risk. And that affects every economic sector. That is not just the software industry. That is every economic sector in the world.

I will just close by saying briefly, beyond the business effects, there are enormous societal benefits that are coming from things like data analytics, from forecasting cholera outbreaks to saving the lives of premature babies to helping farmers reduce use of pesticides. But it is a very new industry, and I think the shadow that the Safe Harbor decision casts over a nascent industry is potentially very damaging.

Mr. WELCH. OK. Thank you. I only have time for one more question, but thank you. I consider that a call to action, Mr. Chairman.

Dr. Meltzer, the dispute here, how much of it has to do in your view with the revelations by Snowden where, on the one hand, that raised questions about the privacy of information that was accessible to national security authorities here, but in Europe we are being told that in fact the security agencies there do the same but with less protections?

Mr. MELTZER. Certainly, the Snowden revelations have cast a significant pall over the entire political discourse in Europe around this issue. There is generally large mistrust in a number of member states about the way that the U.S. Government accesses personal data, and it is not well understood about the progress that has been made in the last couple of years to change that balance. So I think getting that right has certainly been part of it.

It is actually the case that this is a strange debate in Europe to the extent that the national security agencies are not part of the discussion here, and so the balance in the U.S. between innovation, privacy, and that issue is being reflected very differently in Europe.

Mr. WELCH. OK. Thank you. I yield back.

Mr. BURGESS. The gentleman yields back. The chair thanks the gentleman.

The chair recognizes the gentleman from Ohio, Mr. Latta, the Vice Chairman of the Communications and Technology Subcommittee, 5 minutes for questions, please.

Mr. LATTA. Well, thanks very much, Mr. Chairman, and again to our witnesses, thanks very much for all of the information you have given us today. It is very enlightening.

Because when we are talking about trade, it is important to all of us. I visit a lot of my businesses in my district all the time, and small businesses especially, it is amazing how many of them are telling me that they are looking at overseas to find more job creation for at home and then sell their products abroad. So this is very, very important to them to make sure that they can get their products out. And it is also making sure that they keep the people employed.

If I could ask Mr. Murphy, again, we have been talking about this. I know the gentleman from New Jersey was also talking about it a little bit ago that when the European Court, you said, did not examine the recent change in the U.S. oversight electronic surveillance, and you get into the essentially equivalent to the safeguards that exist in the E.U. What we have to do right now to get the Europeans convinced that we are going to have that, essentially the equivalent for our businesses to be able to work with them overseas right now?

Mr. MURPHY. Well, more than anything I think we can do on this side of the pond, it is what we are seeing European business do because if failure to achieve a new Safe Harbor agreement is bad for American business, it is far worse for Europe. According to ECIPE, the European Centre for International Political Economy, the think tank in Brussels, they conducted a study which found that complete data localization in Europe, which is obviously the worst possible outcome of the controversy today, would cost the European economy 1.3 percent of GDP. That is more than $200 billion.

It would mean higher costs for European consumers. As competition is lessened, small businesses in Europe would be particularly

hard hit, as I think we have discussed, in a number of ways here. Some of the smaller E.U. member states would be particularly sidelined. You think about major service providers of digital services that are provided to companies and consumers, in many cases they might simply overlook some of the smaller member states.

We are often hearing from our European friends that they want to develop their own Silicon Valley. They lament that for some reason the U.S. economy is much more innovative. We have an ICT sector in this country that is growing and growing and why can't they achieve it. Well, this kind of ruling could have a very chilling factor. And we should care about that because Europe is our number one economic partner by far, and if their economy, which is experiencing quite slow growth today, a failure to find a path forward here would be very costly for the American economy as well.

Mr. LATTA. Thank you.

Mr. Meltzer, if I could turn to you, and again, your testimony and also what you have written in your testimony that when you look at the internet commerce in the United States grew from over 13 billion in 2011 to the estimate of about 133 billion in 2018 we are seeing what is happening out there. But another question is, will the invalidation of the Safe Harbor agreement indirectly impact trade relations in economies of countries that are outside the E.U.?

Mr. MELTZER. I think potentially, yes, absolutely it will be through a variety of mechanisms. One of them certainly is the fact that trade and commerce now happens in the context of global value chains. So a lot of the cross-border data between the U.S. and the E.U. is in fact incorporating imports and products from around the world, certainly from our NAFTA partners but more globally. And so the impacts and the flow-through of reductions in transatlantic trade investment is going to have global implications at that level.

More broadly is how this privacy debate, I think, plays out globally, whether in fact the world moves down an E.U. top-down privacy approach or adopts more of the U.S. bottom-up company-led sectorial approach is going to, I think, have a broader implications for the types of business models and trade flows that happen globally and will have significant implications for the U.S. going forward.

Mr. LATTA. Let me ask a follow-up on that, then. What should the U.S. Government be doing right now to preempt the problems that could exist then for these countries outside the E.U. because of the decision?

Mr. MELTZER. I think one of the main efforts by the U.S. Government has been in the APEC context, the cross-border privacy principles there, which has been a set of principles around privacy, really quite similar to the ones that the E.U. has. On the principle level there is not that much disagreement. It is really about how they are going to apply it and enforce, whether in fact businesses take responsibility for the privacy of the data or ultimately it is going to be up to sort of a more regulatory government approach to make sure that that happens.

Now, the differences cannot be so great even on that front, but that model, the APEC approach, is the one that the U.S. has been

trying to push through APEC and through other trade agreements in another forum.

Mr. LATTA. Well, thank you very much. Mr. Chairman, my time has expired and I yield back.

Mr. BURGESS. The chair thanks the gentleman. The gentleman yields back.

The chair recognizes the gentleman from Illinois, the subcommittee chairman of the Environment and the Economy Subcommittee, 5 minutes for questions, please.

Mr. SHIMKUS. You forgot to say the powerful chairman of the Environment and the Economy.

Welcome. We are glad to have you here. I am going to be brief. I know my colleagues want to ask a few more questions, and we are kind of beating a dead horse.

I just wanted to say, first of all, we need to get to Safe Harbor 2.0 as soon as possible. And we really can't move to data localization. It will hurt all these things on commerce not just for big businesses but individual consumers. If you look at banking transactions or you are looking at obviously information, engineering data going back, so I am not sure that the public understands the enormity of this issue, and so we want the Administration to keep moving forward possibly in this realm.

But I am always curious about the court ruling and the European community not looking to their own backyard, and to the fact that I think the French new national security surveillance protocols are much more intrusive, and the proposed U.K. could be just as bad on the issues of privacy. So, Dr. Meltzer, can you talk about that little bit? And are they more intrusive in how they might differ?

Mr. MELTZER. I think we are seeing in France following the attacks, the Charlie Hebdo attacks and the attacks on the Jewish supermarket, that there have been proposals to reinvigorate and strengthen the way that the national security agencies operate in France, and certainly some of the proposals there would see collection of data and due process, which would be less than what you see in the U.S.

I think the point is that each country has got to find its own appropriate balance between national security and privacy. The U.S. is clearly going for a revision of that balance here following the Snowden leaks. The problem I think in the debate is that the way that discussion is playing out is that we have a separate debate on privacy as a human right when we talk about this between the U.S. and the E.U., and it ignores the security dimension to these, which is happening at the national member state level.

Mr. SHIMKUS. But they are member states of the E.U., so it is curious for many of us to say it is oK for them locally within their own own country, but as a member of the E.U. to place these additional barriers or concerns or disrupt trade when internally they may be as——

Mr. ROTENBERG. Mr. Shimkus——

Mr. SHIMKUS [continuing]. I want to continue. One more question for Dr. Meltzer, and I did want to be brief. Can you talk about the—Dr. Meltzer, back to the major part of the economy. Any parts

of the economy that would not be affected if this Safe Harbor ruling stays in place?

Mr. MELTZER. Most certainly, I think this point has been made and is worth reinforcing that this is very much an economy issue. This is not a digital economy issue. This is not an IT economy issue. The advanced economies of the United States and Europe are increasingly digital in their entirety, whether we are talking about manufacturing sector, services sector, and certainly the IT sector, the automobile sector, you name it. So there is no area that would not be affected by it.

Mr. SHIMKUS. Thank you, and I want to yield back my time. Thank you, Mr. Chairman.

Mr. BURGESS. The gentleman yields back. The chair thanks the gentleman.

The chair recognizes the gentleman from Kentucky, Mr. Guthrie, 5 minutes for questions, please.

Mr. GUTHRIE. Thank you, Mr. Chairman. I appreciate you all being here. I was just in a meeting with our NATO Alliance members, Members of Congress, parliaments from NATO Alliance, and although we were talking about defense issues in our meetings, almost every time we were walking in or out or just coffee breaks, whatever, the European parliamentarians were very interested in talking about this issue. So it is important here, it is important there, and everybody is focused on that, so I would bring that up.

But, Ms. Espinel and Mr. Murphy, I have a few questions. Do you have member companies that are headquartered in the E.U. but have operations, subsidiaries, or other investment vehicles in the U.S.? And if so, how has this decision impacted their business operations?

Ms. ESPINEL. We do have members that are headquartered in the United States, and we also have members with significant operations in the United States. But I would say for our members, regardless of where they are headquartered, the risks are the same. Our members, regardless of where they are headquartered and the customers that they serve, need data to be moving back and forth across borders. So I think regardless of where—the world that we live in today, regardless of where you are headquartered, I think the risk of the Safe Harbor revocation or the risk of a world in which data cannot move freely back-and-forth are the same.

Mr. GUTHRIE. Thank you. And, Mr. Murphy?

Mr. MURPHY. Just very briefly, we have many members that our U.S. affiliates of European multinationals, and they are just as concerned as the American companies. They see no upside in this. It doesn't provide some kind of a competitive advantage for them to have this kind of forced localization, which would be the worst possible outcome of the failure to renegotiate Safe Harbor. So there is common interest in securing a path forward here.

Mr. GUTHRIE. All right. So, Mr. Murphy, I will ask this to you then. So data localization proposals have been considered in a number of countries in the past 3 years. This topic was the focus of another meeting of this subcommittee. What has your experience been with the challenges these types of proposals pose to the economies in today's global marketplace? Cross data flows have inter-

national implications. Kind of elaborate what you were just saying, I guess.

Mr. MURPHY. Yes. In more than a dozen countries around the world we have been active in trying to reach out to foreign governments to explain to them why data localization is not in their interest. As I mentioned earlier, there is nothing more common than receiving a head of state at the U.S. Chamber of Commerce who says we want to create our own Silicon Valley. The idea of putting up protectionist walls that are going to somehow force the location of servers in the country or the use of domestic-created technologies is really the worst possible prescription for them to be able to do that and do so in a globally competitive manner.

So there have been victories in the past couple of years. For instance, the Brazilian Government considered measures that they later rolled back after hearing from businesses around the world, and it has been quite a constructive relationship. But we continue to see these issues pop up in market after market.

Mr. GUTHRIE. Thanks. I have one more question for you, and if Ms. Espinel will comment as well.

So first, Mr. Murphy, how would you describe the FTC as an enforcement agency for the Safe Harbor? And how do FTC enforcement actions modify business behavior in the U.S.? And do you see any differences in E.U. system that we should be aware of? And, Ms. Espinel, if you will comment after he goes.

Mr. MURPHY. Yes. Well, the U.S. has one of the strongest systems of enforcement led by the FTC, and it has powers and penalties that are significantly stronger than its counterparts in the European Union, including 20-year consent decrees. We think that many of our friends in the European Union don't take that into account, and in particular, don't take into account how these laws are actually enforced, whereas with some other countries that may replicate an E.U. member state law, they would accept their practices as somehow superior to those of the United States, even if enforcement is not nearly on the same level.

Mr. GUTHRIE. Thanks. Ms. Espinel?

Ms. ESPINEL. I would just say, you know, I think at a fundamental level the systems and certainly the focus on privacy between the United States and Europe are not that different, but one of the things that is different about our system is the enforcement authority of the FTC. And I would say on behalf of the software sector we have seen the FTC increasing its enforcement authority and using it in ways—and we think that those are positive steps.

We do think, as has been alluded to earlier today, that there may not be a full understanding on the other side of the Atlantic of the improvements that have been made in our privacy system, including FTC enforcement. I think that is something we need to collectively try to address.

But to your basic question, we are supportive of FTC enforcement, and we have been seeing more of that over recent years, and we think that is a good development.

Mr. GUTHRIE. Thank you. And I yield back the balance of my time. I appreciate it.

Mr. BURGESS. The gentleman yields back. The chair thanks the gentleman.

The chair recognizes the gentleman from Mississippi, Mr. Harper, 5 minutes for questions, please.

Mr. HARPER. Do you need to say Mississippi again, Mr. Chairman? Did you get that?

Mr. BURGESS. [Nonverbal response.]

Mr. HARPER. Thank you. And thanks to each of you for being here today. This is a critically important topic, and to discuss this is very important.

And, Ms. Espinel, if I could ask you first, can you explain how the United States can make the case that we offer essential equivalence in terms of data protection currently?

Ms. ESPINEL. So, I would say a couple of things. I think in terms of—as we said before, I think our immediate goal is to try to get a new Safe Harbor, and I think that is a step that the European Commission can take if they choose to do so. And we are optimistic that they will choose to do so.

But in looking at the long term, essential equivalence or the appropriate standing for privacy protection, that is something that is going to continue to evolve, so that is our opinion, as laws and practices change around the world. And so what we need for the long term is we need a system that is flexible enough. We believe we need a system that is based on principles as opposed to prescriptive regulations. And we need a system that recognizes the importance of privacy. And again, I don't think the differences there between the United States and Europe are that great, but also creates a framework so that a person's personal data will attract the same level of detection as it moves around the world. I think that is something that is important to the United States, as well as Europe.

And we need to be able to find the right balance. We need to let law enforcement do the job that it has to do. And you will not be surprised to hear, on behalf of the business community large and small, we need to have a system that will reduce the legal uncertainty of the situation that we face today.

Mr. HARPER. OK. And of course the challenge for us is to make sure that the rules and regulations don't get in the way of the technology that seems to move at a much faster pace on occasion. So it is a challenge for all of us to go there.

Mr. Murphy, if I could ask you, and I know following up on what has been discussed, what you have mentioned, the ECJ ruling puts some European businesses who transfer data to American companies at risk as well. Could you discuss further whether European businesses have any incentive to put pressure on the U.S. and the Commission to come to an agreement on the Safe Harbor, and if so, how?

Mr. MURPHY. Well, thank you for that question. Many of our sister associations on the other side of the Atlantic are hard at work reaching out to the European Commission and to member state governments urging them to find a path forward as well. If there is one thing that businesses of all sizes dislike, it is uncertainty, and the reach of the ruling that came out in early October was significantly further than anything that was anticipated. And the absence of any kind of a clear transition plan, guidance to companies on how they should behave in the interim while—plus, potentially,

this new Safe Harbor agreement is concluded, has caused real concern across companies in Europe as well. So we have encouraged them to make their voices heard in Europe, as we are doing here.

Mr. HARPER. Thank you, Mr. Murphy.

With that, I yield back, Mr. Chairman.

Mr. BURGESS. The gentleman yields back. The chair thanks the gentleman.

The chair recognizes the gentleman from Texas, Mr. Olson, 5 minutes for questions, please.

Mr. OLSON. I thank the chair. And welcome to all four witnesses.

In many ways, Europe is following Rahm Emanuel's—President Obama's first chief of staff—lead. He said, "you never want a serious crisis to go to waste." The difference is this is not a serious crisis. It is a problem. Again, it is not a serious crisis. It is a problem that will be a crisis unless we fix it by January 31 of next year.

Mr. Murphy, Ms. Clarke brought up the BCRs, the binding corporate rules, also the model contract clauses. Companies have those in effect right now. How are they impacted by the ECJ decision with their data?

Mr. MURPHY. How——

Mr. OLSON. How are they impacted? How are the contract clauses and the binding corporate rules—companies have those. Their data, how is it impacted by the ECJ's ruling?

Mr. MURPHY. Well, these mechanisms were not invalidated by the ruling. However, they are practically out of reach for so many different companies. And as was mentioned earlier, the expense of $1 million and the time it takes, 18 months, to negotiate a new one has made them really impractical for many companies to consider this as an alternative. And you might think that in the wake of this ruling that many companies are considering whether and how they can enter into more of these. And it appears that in the case of some large companies, they are definitely examining some of these alternatives going forward. But for the smaller companies, it simply isn't tenable.

Mr. OLSON. Ms. Espinel, care to comment on that issue, the BCRs, the MCCs with your members?

Ms. ESPINEL. So many of our members are looking at various mechanisms to address this, but I would echo what Mr. Murphy said. Despite the fact that the European Court of Justice opinion does not speak directly to things like the model contract clauses, they are first out of reach for many, many businesses around the world.

And second, to us, they do not represent the sort of long-term solution that we need to have, and that is why we continue to focus on the fact that, while we think it is immediate and vital to have a new Safe Harbor in place and then have some time for companies to come into compliance with that, we need to have a long-term solution that moves beyond things like model contract clauses so that we do not find ourselves in this situation again a year or two down the road.

Mr. OLSON. One final question for all witnesses, the ECJ's decision may open up liability for data transfers from Europe to America for the entire period of the 15 years of Safe Harbor. A Bloomberg article says we may be exposed to liability. My question

is, is that real, Ms. Espinel? Is that a real issue out there? Can 15 years be thrown away with this court decision, exposed liability, American companies, European companies?

Ms. ESPINEL. I think there is a real risk there. However, I would echo what you said. I think what we are facing right now is a significant problem, not a crisis, and I say that in part because we are confident that the United States and Europe will be able to come to a sensible resolution and conclude a Safe Harbor and avoid that situation.

Mr. OLSON. Dr. Meltzer, your comments, sir?

Mr. MELTZER. Let me just say briefly on your question about BCR and contracts, I agree with what the panelists have said. It is worth noting that data protection authorities in Germany have specifically said that they do not think that BCRs and contracts are legally viable mechanisms any longer. The concern obviously is that the structural problems that the European Court of Justice has found with the privacy regime here in the United States is broadly applicable to contracts and BCRs as well. So the issues there make these other mechanisms also unstable.

Mr. OLSON. Thank you. Mr. Rotenberg, the question about liability thrown out for——

Mr. ROTENBERG. Yes, Mr. Olson, I don't think there would be retroactive application of the Safe Harbor decision for prior data transfer, so the short answer is I don't think that risk exists.

However, I think there is another risk to be aware of, which is that this January 2016 deadline that people are talking in terms of presumes that the Article 29 Working Party can keep all of the data protection officials in Europe in check. And all of those national officials have independent authority, so it is actually possible that at any time over the next few months there could be an enforcement action after the Schrems decision became final.

Mr. Murphy, data for the last 15 years of our Safe Harbor, some sort of liability for those?

Mr. MURPHY. I don't have an answer for you, but certainly, this is precisely the sort of uncertainty that alarms corporate counsel and companies across the country.

Mr. OLSON. I thank the witnesses. I ask unanimous consent to enter the article from Bloomberg in the record. And, Chairman, I yield back.

Mr. BURGESS. Without objection, so ordered.

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

Mr. BURGESS. The chair recognizes the gentleman from Kansas, Mr. Pompeo. Thank you for your forbearance, and you are recognized for 5 minutes for questions.

Mr. POMPEO. Thank you, Mr. Chairman.

I want to try and clear away some of what I think are the underlying facts. We have talked a lot about policy. I want to make sure we have got, as best I can, some basic facts in place.

Ms. Espinel, maybe we will start with you. Your companies' data, if the data belongs to a U.S. person or a non-U.S. person, do your companies treat that data any differently?

Ms. ESPINEL. Our companies put the highest level of protection and security on all of their customers' data, regardless of the nationality.

Mr. POMPEO. Right. So they treat it identically. Mr. Murphy, same for yours? It doesn't matter whether a U.S. person or—the data is treated identically?

Mr. MURPHY. Absolutely.

Mr. POMPEO. The same protections? We could go look at the record. I have heard the word privacy concerns uttered maybe 50 times this morning. Concerns are one thing. Ms. Espinel, is there any evidence of abusive practices from U.S. companies with respect to handling PII of either U.S. persons or non-U.S. persons? We have data breaches, we have data get out. I get that. But yes, to you.

Ms. ESPINEL. So I will speak on behalf of my members. Our members are not abusing the data of their customers.

Mr. POMPEO. Right. They are doing their best to protect it. Mr. Murphy, I assume yours are as well?

Mr. MURPHY. That is certainly my impression. And the potential reputational damage from failure to do so is, I think, a powerful factor in their consideration.

Mr. POMPEO. I completely agree. And let's talk about reputational damage actually. Mr. Rotenberg in his written testimony in the summary said "transatlantic data transfers without legal protections were never safe." Mr. Murphy, do you think that is true? Do you think these data transfers have been performed in an unsafe manner?

Mr. MURPHY. No, I think that it has been a 15-year record of success and really comparable in success to that related to data transfers within Europe between member states.

Mr. POMPEO. Ms. Espinel, would you agree with that?

Ms. ESPINEL. Speaking for the members that I represent, yes, I would agree with that.

Mr. POMPEO. So I think it is that kind of hyperbole that has caused the European elected officials to have no backbone on this issue. I get the politics, I get the protectionism. I completely understand how they have all watched the Snowden hearings and decided they could get elected but didn't defend the privacy actions that are taken by your companies. We have had talk today about Section 702. Mr. Murphy, do any of your clients ever collect data under Section 702?

Mr. MURPHY. I just have no information on that.

Mr. POMPEO. Yes. Ms. Espinel, do you know?

Ms. ESPINEL. I don't. But what I would say is that we have made this point in the hearing before. I think one of the things that is crucial here is that there is a real lack of understanding on both sides of the Atlantic, but I think the Europeans, both on privacy regimes but also, as was touched on earlier, the complications of our various surveillance regimes. And one thing that I don't think has been done but I think be very useful is to have a comprehensive analysis of the surveillance regimes across the European Union states because I don't think there is a good and clear understanding, and I think that has led to a lot of confusion, you know, deliberate or not.

Mr. POMPEO. Yes, I think that is not lack of understanding. I think that is willful ignorance. But maybe we disagree.

Mr. Rotenberg, I want to make sure I understood something you said. You talked about Section 702 a bit. I know a little bit about it but maybe you know more. Is it your position that U.S. persons and non-U.S. persons should be treated identically with respect to the U.S. Government collection of information?

Mr. ROTENBERG. I think under the Foreign Intelligence Surveillance Act there is a clear distinction——

Mr. POMPEO. No, I am asking if you think. You have suggested a modification to U.S. law. That is U.S. law. I guess my question is, is it your position or your organization's position that U.S. persons and non-U.S. persons should be treated identically with respect to government information collection?

Mr. ROTENBERG. As a general matter, yes. And most of U.S. privacy law takes that position, particularly on the commercial side. There is no distinction in our commercial privacy law——

Mr. POMPEO. Yes.

Mr. ROTENBERG [continuing]. Between U.S. persons and non-U.S. persons.

Mr. POMPEO. Fair enough. Just so you know, that would be historic. You could very well be right about it being proper, but no nation has ever behaved that way with the collection of data for their own citizens as against the others. There is always a wrinkle. There is always an exception. There is always a Section 1233, executive order. There is always a way that nations have, in their efforts to provide national security for their own people, have behaved that way. And I actually think the United States has done a remarkable job of protecting citizens all around the world and protecting their data in their efforts to keep us all safe. I think that is important.

Mr. ROTENBERG. Sir, may I ask, do you think that the Office of Personnel Management has done an excellent job protecting the records of the federal employees——

Mr. POMPEO. Well, no, sir. There are errors all along the way. I am asking——

Mr. ROTENBERG. Twenty-one-and-a-half million records——

Mr. POMPEO [continuing]. About policy. I am asking about policy and——

Mr. ROTENBERG. SF–86, those——

Mr. POMPEO. Yes.

Mr. ROTENBERG [continuing]. Are the background investigations——

Mr. POMPEO. Very familiar with that. I filled one out and I think mine was released as well, sir, so I am intimately familiar with that. I didn't say we didn't have errors and mistakes. I am simply talking about policy.

Let me ask one more question. Mr. Murphy, you talked about this million-dollar cost for private solutions, these BCRs or other delegated methodologies. Is there any way to drive that cost down? Is there any way to make that a hundred-thousand-dollar cost instead of a million-dollar cost?

Mr. MURPHY. Not substantially. And I think that as we look at some of these alternatives like BCRs to the degree that they do continue to be relevant going forward, it is a field day for lawyers.

And I suppose there is some job creation in that. But that is clearly not the intention of the policy.

Mr. POMPEO. Thank you. I am past my time. Thank you for bearing with me, Mr. Chairman. I yield back.

Mr. BURGESS. The chair thanks the gentleman. The gentleman yields back.

The chair recognizes the gentleman from Florida, Mr. Bilirakis, 5 minutes for your questions, please.

Mr. BILIRAKIS. Thank you, Mr. Chairman. I thank the panel for testifying.

This issue arose quickly, and I am glad we are addressing it today so that some certainty can be given to the numerous businesses seeking answers as they tried to continue the pursuits in a global marketplace.

Ms. Espinel and Mr. Murphy, I know you touched on this a bit, but what challenges are companies facing as they evaluate and even implement the other mechanisms in the E.U. that permit data transfers to countries outside the E.U.?

Ms. ESPINEL. So one specific challenge that companies are facing, big companies and small companies, is the processing of their payroll and making sure that their employees get time. If there is not a resolution of the Safe Harbor, that is something that could be at risk. And that is obvious business disruption, but it is also disruption to the lives of human beings that are employed by those companies.

Let me mention one thing that I haven't mentioned before. We did a survey last year, which I would be happy to share, where we talked to the CEOs and senior executives of companies in the United States and Europe in terms of what data meant to them and how valuable it was to their business. And one of the things that was really surprising to me is really small companies, companies that have less than 50 employees, already today find data enormously important to going into new markets, serving their customers, developing new products. What I found less surprising is that that is true on both sides of the Atlantic. So for U.S. companies and for European companies the ability to move data back and forth in order to do business is critically important.

Mr. BILIRAKIS. Thank you, Ms. Espinel.

Mr. Murphy?

Mr. MURPHY. Well, a little to add but I would just—to recapitulate one point, the morning the ruling came out I think many of us were just disappointed at the lack of any guidance that came out from the European Commission. And there has been a little more since then, but that is exactly the kind of uncertainty that serves as a wet blanket on the economy at a time when not only is the U.S. economy not growing as rapidly as we would like, but in Europe, far worse. And it is the last thing that the global economy overall needs right now.

Mr. BILIRAKIS. Well, thanks so much. Another question for you, Mr. Murphy. What impact does the European Court of Justice ruling have on the negotiations of other large-scale international trade agreements like the TPP and the T2?

Mr. MURPHY. So the United States and the European Union are 2 years into negotiating a comprehensive Transatlantic Trade and

Investment Partnership agreement. These negotiations are still at a relatively early stage despite the length of time involved. This kind of a ruling, though, it does certainly put a damper on the mood in the room. After all, the TTIP, as that negotiation is called, is intended to safeguard not just the movement of goods and services across international borders but also data as a trade issue.

U.S. trade agreements, including the TPP, have strong measures to prohibit the forced localization of data. And of course, privacy regimes coexist with those trade obligations. And privacy obligations are not undermined by the trade agreements.

But the situation we have right now with the invalidation of the Safe Harbor agreement certainly has led some to question the seriousness with which we can move forward in those negotiations.

Mr. BILIRAKIS. So there are some national security concerns until the Safe Harbor agreement is signed?

Mr. MURPHY. Well, certainly for commercial data and the ability to move it across border, that is very much a concern.

Mr. BILIRAKIS. Thank you. Thank you.

Dr. Meltzer, what impact has the global reach of the internet had on small and medium-sized businesses? You mentioned in your testimony that they are underrepresented in international trade. Is this just a function of their size or can we incentivize small- and medium-sized businesses in international trade agreements going forward?

Mr. MELTZER. Traditionally, SMEs have not made big plays in the international economic landscape. It has been for a variety of reasons to do with cost and capacity. The internet has certainly changed that for them. The International Trade Commission did an interesting study which found that access to information, for instance, about overseas markets has been one of the key barriers for small- and medium-sized enterprises. In just thinking about going global, the cost of getting that information is obviously now close to zero. That is just one example of the many ways that internet and internet platforms are now providing new opportunities for SMEs to be part of the global economy.

Mr. BILIRAKIS. Thank you. I yield back, Mr. Chairman. I appreciate it.

Mr. BURGESS. The gentleman yields back. The chair thanks the gentleman.

The chair recognizes the gentlelady from Indiana, Mrs. Brooks, 5 minutes for questions.

Mrs. BROOKS. Thank you, Mr. Chairman.

My home State of Indiana has a large contingent of pharmaceutical and device companies who depend on the Safe Harbor to transfer, and I believe we have talked about the issues of big data and those companies that are using big data. Companies like Eli Lilly use the cloud-based software for the users, can share of medical images with other departments and centers and countries around the world to improve the product design, to allow for nearly instantaneous interpretation and diagnosis of medical records, and compile records for clinical studies.

And we certainly know that the utilization of cross-border data enables all of our life sciences companies in the country to use these data sets so we can get treatments and that we can improve

faster development of treatments and diagnoses and better health care for not just those in the U.S. but for the world. So I certainly recognize the anxiety everyone is having at this point in time based on the ECJ decision.

But I am curious, what do you think we should be watching in these next few months as this January 2016 deadline is approaching? What should we be watching and what—there has been dialogue about this with our government and with the E.U. members for years now. I actually participated in one of those discussions in late 2013 in Brussels with some other Members of Congress, a bipartisan delegation, but yet, it does not seem as if we have bridged the gap of either trust or of understanding. And I am curious what you all believe we need to be doing a better job of doing to either get to a Safe Harbor agreement 2.0.

And my second question is why do we believe that the court will even agree or why do we believe it would even be upheld and not challenged immediately again? And I guess I would like to hear each of your comments. Ms. Espinel?

Ms. ESPINEL. So in the short-term, as you say, I think we need to focus on concluding the Safe Harbor. The kind of discussion that you were having with your European counterparts I think is really important. I think having hearings like this that focus on the issue is really important. I think if we are going to be able to make progress both in terms of concluding in the short term the negotiations and the longer-term solution, we need to have a constructive political environment. And part of the way that we get there is by having Congress in contact not just with the Administration but also with your European counterparts both to help them understand our privacy system better and understand the improvements that have been made in that privacy system. I think that is a really important role that Congress can play both in the short term and over the longer term.

Mrs. BROOKS. So I attended with the chair of the House Intelligence Committee, Chairman Rogers and the ranking member, Ranking Member Ruppersberger, in this delegation meeting. Are you familiar with other conversations? That was in 2013. And are you familiar with other conversations that Members of Congress have had or that—because it is clear to me that what the negotiations and the discussions between the Administration officials, it is not working.

Mr. ROTENBERG. Right——

Mrs. BROOKS. So where are we falling down?

Mr. ROTENBERG. Let me begin by saying I actually think Congressman Sensenbrenner deserves a lot of recognition——

Mrs. BROOKS. Yes.

Mr. ROTENBERG [continuing]. For the work that he has done on this issue. I think it is one more demonstration of how privacy really does cross the aisle. And I know he has expressed concern about making changes to 702, and that is one of the issues that we think does need to be addressed.

But I think it is also important in the context of this hearing to understand that there is a difference between the political negotiation that takes place between the U.S. Commerce Department and the European Commission and a judicial decision from the top

court in Europe. I mean this really is a game changer, and it impacts what even the European Commission can do in its negotiation with the United States. So to your question, I think it will be very interesting to see over the next few months how this change in European Union law, which is what has happened, will influence the privacy officials across Europe. They may decide to take enforcement actions.

Mrs. BROOKS. Mr. Murphy?

Mr. MURPHY. I think one of the most important things that Members of Congress can do is to educate their European counterparts on the importance of these data flows. And coming back to your example about medical devices, just yesterday, we were hearing from one of our member companies that manufactures medical devices, and some of these, such as different scanners, CAT scanners, PET scanners, MRIs are very large, expensive, sophisticated pieces of equipment. In some smaller E.U. member states there may be only a very small handful of them around. And they are often maintained and used remotely. That is another example of the kind of data which needs to flow.

And talk about taking the whole to date to a very personal level, that the ability to get this kind of medical information, the idea that it could be impeded by a failure to arrive at a new Safe Harbor agreement is something that I think all of us find concerning.

Mrs. BROOKS. Thank you. I yield back.

Mr. BURGESS. The gentlelady yields back. The chair thanks the gentlelady.

The chair would just ask, are there any other Members seeking time for questions?

Seeing none, I do want to thank our witnesses for being here today. Before we conclude, I would like to submit the following documents for the record by unanimous consent: a statement from the International Trade Administration at the United States Department of Commerce, a letter from the Direct Marketing Association, a statement from the Information Technology and Innovation Foundation, a statement from the American Action Forum, a joint letter from the Auto Alliance, American Automotive Policy Council, and Global Automakers, and a list of all of the 4,400 United States companies who are active beneficiaries of the Safe Harbor agreement. [1] I will not read them unless asked.

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

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

Without objection, the subcommittee stands adjourned.

[Whereupon, at 12:17 p.m., the subcommittees were adjourned.]

[Material submitted for inclusion in the record follows:]

---

[1] The list has been retained in committee files and is also available at *http://docs.house.gov/meetings/if/if16/20151103/104148/hhrg-114-if16-20151103-sd015.pdf*.

Internet Association

The Honorable Michael Burgess
Chairman, Commerce, Manufacturing, and Trade Subcommittee
United States House of Representatives
2125 Rayburn House Office Building
Washington, DC 20515

The Honorable Greg Walden
Chairman, Communications & Technology Subcommittee
United States House of Representatives
2125 Rayburn House Office Building
Washington, DC 20515

The Honorable Jan Schakowsky
Ranking Member, Commerce, Manufacturing, and Trade Subcommittee
United States House of Representatives
2125 Rayburn House Office Building
Washington, DC 20515

The Honorable Anna Eshoo
Ranking Member, Communications & Technology Subcommittee
United States House of Representatives
2125 Rayburn House Office Building
Washington, DC 20515

Examining the EU Safe Harbor Decision and Impacts for Transatlantic Data Flows

Chairmen Burgess and Walden and Ranking Members Eshoo and Schakowsky:

The Internet Association writes to express our views on recent events impacting the U.S./EU Safe Harbor. Cross-border data flows between the U.S. and Europe are the highest in the world and the free movement of data creates jobs and enhances growth on both sides of the Atlantic.[1] It is therefore imperative that data flows between the U.S. and the EU be supported in a way that provides legal certainty and continuity to businesses and consumers alike.

The Internet Association is the unified voice of the Internet economy, representing the interests of leading Internet companies[2] and their global community of users. The Internet Association is dedicated to advancing public policy solutions to strengthen and protect Internet freedom, foster innovation and economic growth, and empower users. Important to our mission is the advancement of public policies that support the free flow of data globally while promoting and protecting privacy. Until recently, the U.S./EU Safe Harbor framework served both these policy goals effectively. Over 4,400 US companies relied on Safe Harbor to validate the transfer of data from the EU to the U.S., including both U.S. headquartered companies and U.S. based subsidiaries of EU headquartered companies. Over half of these companies are small and medium sized enterprises.

---

[1] Joshua Meltzer, *The Importance of the Internet and Transatlantic Data Flows for U.S. and EU Trade and Investment*, Global Economy and Development at Brookings Research Paper (Oct., 2014), http://www.brookings.edu/research/papers/2014/10/internet-transatlantic-data-flows-meltzer.

[2] The Internet Association's members include Airbnb, Amazon, auction.com, Coinbase, Dropbox, eBay, Etsy, Expedia, Facebook, FanDuel, Gilt, Google, Groupon, Handy, Intuit, LinkedIn, Lyft, Monster Worldwide, Netflix, Pandora, PayPal, Practice Fusion, Rackspace, reddit, Salesforce.com, Sidecar, Snapchat, SurveyMonkey, TripAdvisor, Twitter, Yahoo, Yelp, Uber, Zenefits, and Zynga.

1333 H Street NW, Washington, DC 20005
12th Floor, West
www.internetassociation.org

Internet Association

Like the thousands of U.S. and EU companies who complied with the Safe Harbor in good faith, our members were disappointed when the European Court of Justice recently invalidated the Safe Harbor effective immediately. While the Internet Association respects that ECJ opinion in the Schrems case as binding and final in nature, we think it important to flag two issues with the court's analysis of U.S. law since they should be factored into the ongoing negotiations between the EU and the U.S. around the renewed Safe Harbor framework. These two issues are the court's analysis of U.S. surveillance law as well as its treatment of U.S. commercial privacy law in the Schrems opinion.

First, the ECJ Schrems opinion is premised on inaccurate assumptions about U.S. surveillance law that do not capture the significant surveillance reforms undertaken since 2013. The Internet Association and its members have consistently supported these reform measures, which should inform negotiations to revitalize Safe Harbor.

In the aftermath of the Snowden revelations, President Obama's Review Group on Intelligence Communications and Technology drafted a comprehensive report with a set of 46 recommendations concerning reforms to U.S. surveillance programs, laws, and intelligence agencies. Some of these recommendations formed the basis for subsequent legislation while others continue to inform the debate about broader surveillance reform measures. Separately, the Privacy and Civil Liberties and Oversight Board (PCLOB) published comprehensive reports with concomitant recommendations related to key sections of the Foreign Intelligence Surveillance Act (FISA) and the PCLOB is currently undertaking a review of Executive Order 12333.

In June this year, President Obama signed the USA Freedom Act into law. The USA Freedom Act prohibits the bulk collection of telephony and Internet metadata under various U.S. legal authorities, allows companies to publish transparency reports with further granularity around the volume and scope of national security demands issued by governmental entities, and codifies new oversight and accountability mechanisms.

The USA Freedom Act was preceded by Presidential Policy Directive PPD-28. PPD-28 provides that signals intelligence collected about non-U.S. persons may no longer be disseminated solely on the basis that the information pertains to a non-U.S. person. To the extent that signals intelligence is collected about non-U.S. persons in bulk, it must be for one of six specified purposes[3] and no others.

More recently, on October 20, 2015, the House of Representatives passed the Judicial Redress Act (H.R. 1428) by a voice vote. This legislation, if enacted by the Senate, would ultimately enable non-US persons to enjoy judicial redress rights given to U.S. citizens under the Privacy Act of 1974.

Unfortunately, none of these significant changes to U.S, surveillance law and oversight were analyzed by the ECJ in its recent Safe Harbor opinion. Significantly, these undertakings by the U.S. government

[3] Counter-espionage, counterterrorism, counter-proliferation, cybersecurity, detecting and countering threats against U.S. armed forces or allied personnel, and to combat transnational criminal threats.

1333 H Street NW, Washington, DC 20005
12th Floor, West
www.InternetAssociation.org

Internet Association

stand in stark contrast to the ECJ's view that the U.S. engages in "indiscriminate surveillance and interception carried out [] on a large scale."

Separate and apart from surveillance reforms, the ECJ Safe Harbor opinion did not acknowledge today's layered and effective U.S. commercial privacy enforcement regime. Since the late 1990s, the Federal Trade Commission has enforced its broad authority under Section 5 of its enabling statute over 100 times against data privacy and security violations that constitute "unfair or deceptive acts or practices in or affecting commerce."[4] Beyond this broad FTC jurisdiction, Congress has enacted several sector specific statutes protecting children's, financial, and healthcare information. And beyond Congress, the states have enacted over 300 privacy laws controlling a diverse array of issues - from data breach to employer access to their employees' social media accounts.

The U.S. Department of Commerce and European Commission have spent nearly two years renegotiating a renewed Safe Harbor agreement to address the Commission's concerns regarding the protection of EU citizens' privacy since the national security revelations of 2013. The revised framework will strengthen protections for EU citizens' data while facilitating transatlantic data flows that bring significant benefits to the U.S. economy and the EU economy alike.

It is important to the Internet Association that the ongoing Safe Harbor negotiations between the U.S. and the EU are premised on a fair and current understanding of U.S. law. In its Safe Harbor opinion, the ECJ laid out the standard for "adequacy" that would allow for continuing data flows between the EU and the U.S. and we are confident the U.S. regime, when fairly examined, would satisfy this standard. We therefore urge the Department of Commerce and the EU Commission to take into consideration the current state of *both* U.S. surveillance law and commercial privacy law in finding the common ground needed to reach agreement on a new Safe Harbor framework.

We urge the Department of Commerce to conclude the ongoing Safe Harbor negotiations as soon as possible and, in conjunction with the European Commission, announce the revised framework. The announcement of this framework will represent an important step in providing businesses with certainty and stability in their transfer of data across the Atlantic, and will reassure European citizens that their personal data will continue to be afforded the highest level of protection when it is transferred to the United States.

Respectfully submitted,

_____

Michael Beckerman
President & CEO
The Internet Association

[4] 15 USC §45(a).

1333 H Street NW, Washington, DC 20005
12th Floor, West
www.internetassociation.org

EU Safe Harbor Demise Raises Retroactivity Concerns

October 7, 2015 5:04PM ET

Oct. 7 (BNA) -- U.S. companies reeling from the European Union top court's invalidation of the U.S.-EU Safe Harbor Program have another headache—the legal status of data they transferred out of the European Economic Area during the decade-and-a-half-long operation of the program.

Any transfer of data to the U.S. from the EEA in the last 15 years that relied only on the Safe Harbor Program may in principle be open to a legal challenge in the wake of the recent invalidation of the Safe Harbor adequacy decision, the European Commission, the EU's administrative arm, confirmed Oct. 7.

An official from the commission's legal service, speaking on condition of anonymity, told Bloomberg BNA that the European Court of Justice's Oct. 6 invalidation of Safe Harbor applied to past data transfers as well as future ones.

That means any transfer to the U.S. from the EEA—the 28 EU member states and Iceland, Liechtenstein and Norway—that couldn't show reliance on an alternative legal basis "should not have been made," the official said.

A privacy attorney who asked not to be named because of the sensitivity of the issue told Bloomberg BNA Oct. 7 that the retrospective application of the ECJ's invalidation of Safe Harbor was "one of the biggest issues of the decision," and a "crazy, crazy outcome."

The court ruling "raises significant issues of legal uncertainty" because it could, in theory, result in EU data protection authorities being required to consider complaints against any data transfer in the last 15 years, the attorney said.

As If Safe Harbor 'Never Existed.'

The Safe Harbor Program allowed U.S. companies to transfer EU citizens' data to the U.S. if they self-certified to the U.S. Department of Commerce their compliance with privacy principles similar to those contained in the EU Data Protection Directive.

The ECJ, the EU's highest court, Oct. 6 invalidated a European Commission decision from 2000 that found that Safe Harbor provided adequate privacy protections for the data of EU citizens (see related article).

The ECJ held that the commission's decision was invalid because the program didn't safeguard personal data against surveillance by the U.S. government and didn't allow for sufficient redress for EU citizens whose privacy had been breached. In addition, the commission's adequacy finding was flawed because it didn't fully respect the independence of EU national data protection authorities, the ECJ said.

The official from the commission's legal service said that the ECJ's finding that the adequacy decision was invalid "means indeed that the decision is gone as if it never existed."

Howard W. Waltzman, partner at Mayer Brown LLP in Washington, told Bloomberg BNA Oct. 7 that the ECJ's invalidation of the commission finding means companies "can't rely on the decision in and of itself for any transfer."

Under the EU's Data Protection Directive (95/46/EC), the personal data of EU citizens can only be transferred outside the bloc if the jurisdiction the data is being transferred to is judged to offer adequate data protection. Companies may also lawfully transfer personal data through the use of binding corporate rules or model contracts, or under exceptions, including that the data subject provides specific consent or that the data transfer is necessary for the fulfilment of a contract.

Risk of Challenges

The privacy attorney said it was difficult to tell if past transfers made under Safe Harbor would be challenged but that there remained a risk that another individual might raise a challenge, as Austrian law student Max Schrems did in the underlying case against Facebook Inc. that gave rise to the ECJ ruling.

It is likely that EU data protection authorities would be "practical," and there was a "limited risk" that they would start their own investigations into transfers done under Safe Harbor, the attorney said. But any complaint to a DPA might potentially trigger "very tricky questions," the attorney said. It would be difficult to demonstrate a fault when companies had acted in good faith under Safe Harbor, the lawyer added.

Waltzman said that any "retroactive liability" challenge against the validity of a data transfer made under Safe Harbor "would certainly be an interesting challenge in the courts."

Harm Threshold Still in Play

A European Commission official speaking on condition of anonymity at a briefing Oct. 7 said that in case of any legal challenge against a data transfer made under Safe Harbor, a company could defend itself by showing that "at the moment of a transfer" it was using an alternative basis for the transfer allowed under the Data Protection Directive, such as binding corporate rules or model contractual clauses.

The official added that "there are a number of conditions that have to be fulfilled" in any attempt to challenge a past transfer made under Safe Harbor, including a question of whether data subjects faced harm from what would now be considered an unlawful transfer.

The commission official was unable to quantify the proportion of data transfers from the EU to the U.S. that rely only on Safe Harbor as a legal basis. Larger companies are "generally equipped with other bases," such as BCRs, the official said.

However, there was "rapid growth in the number of companies that have participated over the life of Safe Harbor," the official said.

To contact the reporter on this story: Stephen Gardner in Brussels at correspondents@bna.com

To contact the editor on this story: Donald G. Aplin at daplin@bna.com

Electronic Commerce & Law Rep.

International Trade Daily

Privacy & Security Law Report

Testimony of
Edward M. Dean, Deputy Assistant Secretary for Services,
International Trade Administration, U.S. Department of Commerce
Before the House Energy and Commerce Subcommittees on Commerce,
Manufacturing and Trade and Communications & Technology
U.S.-EU Safe Harbor Framework
November 3, 2015

I. Introduction

Good Morning, Chairmen Burgess and Walden, Ranking Members Schakowsky and Eshoo and distinguished Committee Members. Thank you for the opportunity to submit written testimony about the U.S.-EU Safe Harbor Framework. I have welcomed the high-level attention Committee Members have brought to Safe Harbor since the October 6 European Court of Justice (ECJ) decision. Your statements, letters and outreach have highlighted the importance of Safe Harbor to U.S.-EU trade and the need to promptly endorse the strengthened Framework that we have negotiated with the European Commission during the past two years. With over 4,400 companies in the United States utilizing the program, it is a cornerstone of the transatlantic digital economy enabling growth and innovation in the United States and in Europe. As a result, it is my top priority and is a top priority of our Secretary of Commerce and the Administration as a whole.

In my capacity as Deputy Assistant Secretary for Services in the International Trade Administration, I oversee the team administering the Safe Harbor Framework at the Department of Commerce and have led our consultations with the European Commission over the past two years to update Safe Harbor. In this testimony, I will provide a brief history of the Safe Harbor Framework and our engagement with the European Commission. I will then discuss the ECJ decision, its implications and our work to ensure data flows between the United States and EU can continue.

II. History of the U.S.-EU Safe Harbor Framework

The Safe Harbor Framework has, for 15 years, served as a model for the protection of privacy while facilitating data flows that fueled growth and innovation on both sides of the Atlantic. Safe Harbor was developed by the U.S. Department of Commerce and European Commission following the adoption in 1995 of the EU Directive on Data Protection (EU Directive 95/46/EC). The EU Directive came into effect in 1998, restricting the transfer of personal data to non-EU countries that did not meet the EU "adequacy" standard for privacy protection. While the United States and the EU share the goal of protecting the privacy of our citizens, the U.S. approach to privacy, which includes sectoral privacy legislation, state laws, and robust enforcement by the U.S. Federal Trade Commission, has not been deemed adequate by the EU.

In order to bridge these differences in approach and provide a means for U.S.-based companies to receive data from the EU in compliance with the EU Directive, the U.S. Department of Commerce in consultation with the European Commission developed the Safe Harbor Framework. The Safe Harbor Framework was designed as a voluntary, enforceable code of

conduct based on globally-recognized privacy principles to which U.S.-based companies could self-certify. Under Safe Harbor, U.S.-based companies voluntarily certify their commitments to Safe Harbor's data protection requirements. In doing so, those companies' public commitments and attestations became enforceable by the U.S. Federal Trade Commission. The Safe Harbor Framework was deemed "adequate" by the European Commission and EU Member States in 2000. The Department of Commerce has worked closely with the European Commission since the program's inception to strengthen the operation of program within the parameters of the existing Framework.

By the time of the European Court of Justice ruling, over 4,400 companies in the United States were participating in Safe Harbor and relying on the European Commission's determination that it provided adequate protection to process data in the course of transatlantic business. These 4,400 participants come from nearly every sector of the economy. 61% of the companies are small and medium sized businesses with 250 or fewer employees. They include U.S.-headquartered companies, as well as U.S.-based subsidiaries of EU companies. While media focus has centered on data exchanged through social networks and as part of cloud services, Safe Harbor participants process a wide variety of data from Europe to conduct business. This includes human resources data of EU-based employees, shipping and billing information for the purchase of goods and services, and transactional data necessary to support 24/7 customer service. In short, the global trading and financial system today depends on the ability to seamlessly send and receive personal data without regard for national borders. This dependence is revealed by the more than $240 billion worth of digitally deliverable services trade between the United States and Europe. Safe Harbor ensured that this data could move both efficiently and in compliance with EU law.

III. Recent Developments and DoC Engagement

Following the surveillance disclosures in 2013, the European Parliament and some EU Member State officials called for suspension of the Safe Harbor Framework. The European Commission responded with a review of the Framework followed by the release of a Communication with 13 recommendations to improve the Framework. The first eleven related to commercial data flows and the last two pertained to national security issues. Following the release of the Commission's Communication in November 2013, the Department of Commerce initiated consultations with the Commission to address their recommendations.

Before describing the negotiations, it is worth saying a few words about the broader political context in Europe around these issues. Since Safe Harbor had become linked to the surveillance disclosures, it became a target for continued criticism largely based on misunderstanding and false assumptions about its purpose and operation and the important privacy benefits it provided. At their heart, many of these criticisms were based on false accusations that the United States was engaged in "mass, indiscriminate surveillance" of the data transferred to the United States under Safe Harbor.

For the past two years, the Department, along with the U.S. Federal Trade Commission and Department of State, has engaged in consultations with the European Commission. We have also worked with officials from the Intelligence Community and the Department of Justice to discuss the national security-related recommendations. Recognizing the importance of data

flows and the challenging political context in which we were operating, we worked hard to strengthen the framework and address concerns raised in the EU. In our view, it was appropriate to modernize the 15-year old Framework, and there were improvements and changes we could make that enhanced privacy protections while continuing to facilitate data flows. Throughout this process, we consulted regularly with U.S. stakeholders to discuss both the privacy benefits and commercial feasibility of potential changes. We were mindful of areas that might cause new compliance costs for U.S. firms and pushed back in our negotiation when we felt that any change might unduly burden U.S. firms relative to other companies. These were difficult negotiations, but over the summer we reached a tentative agreement that was subject to review and approval by the European Commission's political leadership. At that point, the Commission chose not to move forward given the pending issuance of the European Court of Justice Decision.

In its October 6 ruling, the European Court of Justice invalidated the European Commission's determination in 2000 that Safe Harbor provides adequate protection for personal data. This determination by the Commission was the legal foundation for Safe Harbor. The ECJ decision did not examine or make findings regarding the adequacy of U.S. protections; rather, it faulted the European Commission for examining Safe Harbor but not the broader U.S. legal context in 2000. Unfortunately, the ECJ decision did not allow a transition period for companies to make alternate legal arrangements, creating even greater legal uncertainty.

We are deeply disappointed in the ECJ decision, which creates significant uncertainty for both U.S. and EU companies and consumers, and puts at risk the thriving transatlantic digital economy. The ruling does not give adequate credit for the robust protections of privacy available in the U.S. or all that the Framework has done to protect privacy and enable economic growth. We are focused on and fully committed to resolving the uncertainty that the decision has created and thus end the significant, negative consequences that flow from such uncertainty.

We fully understand how harmful uncertainty can be to a business, its growth, employees, customers, and vendors, and have been hearing directly from companies, large and small, about the real world impact of the ECJ decision. We have stressed to the Commission that real harm is presently being borne by companies that have committed in good faith to protect privacy in accordance with globally recognized principles. It is worth emphasizing that the ECJ decision does not question whether U.S. companies provided their consumers with the protections promised under the Safe Harbor.

To illustrate just how harmful the uncertainty created by the ECJ decision has been, I offer two illustrative examples:

- A small company, which provides support services relevant to clinical research trials, has already lost significant business across Europe. The company's clients are suspending and shutting down projects, while its EU-based main competitor has reached out to other existing clients recommending they switch providers in light of the court ruling.

- A large U.S.-based hotel chain with properties across the EU would in the absence of Safe Harbor have to either: put in place EU model contracts with each of its vendors –

something it described as a logistical nightmare – ; or, take on the EU's binding corporate rules process, which is very expensive and has an 18-month lead time.

While model contracts, binding corporate rules, and other options for compliance with European privacy law do exist, the ECJ ruling has also raised questions about their viability. For example, following the ECJ ruling, a German DPA released a position paper indicating that model contracts and consent might also be considered invalid for transferring data to the United States.

We believe the best way to protect privacy and restore confidence in transatlantic data flows is to promptly endorse and put in place the strengthened Safe Harbor Framework that we have negotiated with the European Commission during the last two years. We have provided a very strong basis for the European Commission to make the findings discussed in the ECJ decision, including on the national security issues. That being said, we are continuing to discuss ways to improve and strengthen the overall package now, and to be sure that it addresses the specific issues raised by the court.

This is a priority for me, for Secretary Pritzker and for the Administration as a whole. We have welcomed many of your own calls for this important step. Secretary Pritzker, senior officials at the White House and across the interagency community have been in close and regular contact with the European Commission, as well as other partners across Europe, including within individual Member States, and have expressed the need for urgent resolution of this issue. I was in Europe during each of the past three weeks meeting with the European Commission, EU data protection authorities, EU Member State officials and affected U.S. and EU businesses to discuss the path forward. Our Secretary, Deputy Secretary, and the Under Secretary for International Trade among other senior officials have also traveled to Europe during this time. Each has engaged on this issue both during their trip as well as from Washington.

IV. Conclusion

We remain committed to doing everything we can, as fast as possible, to move forward with a new Safe Harbor Framework. We are prepared to focus full time on this issue in order to bring greater certainty around the critical issue of data flows. We are hopeful that our partners in the Commission will be willing to approach this with the same sense of urgency, and we appreciate the focus you and your colleagues here in Congress can bring to this important issue.

Christopher Oswald
Vice President, Advocacy

November 3, 2015

The Honorable Michael C. Burgess, M.D.
Chairman
Subcommittee on Commerce, Manufacturing, and Trade
Committee on Energy and Commerce
United States House of Representatives
Washington, DC 20515

The Honorable Greg Walden
Chairman
Subcommittee on Communications and Technology
Committee on Energy and Commerce
United States House of Representatives
Washington, DC 20515

Dear Chairman Burgess and Chairman Walden:

The Direct Marketing Association (DMA) wishes to express its support for continued efforts to successfully resolve the negotiations to create a successor agreement to the now stricken U.S.-EU Safe Harbor. The recent decision of the European Court of Justice (ECJ) to invalidate the Safe Harbor Agreement has increased the sense of urgency around these negotiations, and we thank you for continuing to bring attention to these negotiations by holding this joint subcommittee hearing, "Examining the EU Safe Harbor Decision and Impacts for Transatlantic Data Flows."

Since 2001, the DMA has operated the DMA Safe Harbor Program for its members. Through this program, DMA has served as a recognized independent recourse mechanism available to investigate unresolved complaints from European data subjects. In addition, the DMA has collaborated with business and consumer experts to mediate data privacy disputes and make policy recommendations involving the Safe Harbor Framework. In this role, the DMA has had a unique view of the benefits provided to businesses and consumers by the free flow of information across the Atlantic.

DMA is the world's largest trade association dedicated to advancing and protecting responsible data-driven marketing in the United States and globally. Founded in 1917, DMA represents thousands of companies that drive the information economy. DMA members have

engaged in the responsible collection and use of data for marketing purposes for more than 100 years. These responsible and innovative data uses have revolutionized the delivery of products and services to their customers and fostered many additional consumer benefits, such as virtually limitless free online content and services. According to a recent study, the resulting Data-Driven Marketing Economy (DDME) added $156 billion in revenue to the U.S. economy and fueled more than 675,000 jobs in a single year.[1]

These activities are not strictly geographically limited and contribute to a robust global economy. Research published in July 2012 by the Direct Marketing Association (UK) Ltd revealed a projected growth of 7% in the direct marketing industry in 2012 in the UK, from the £14.2 billion spent in 2011 to nearly £15.2 billion forecast for 2012. UK companies profiled in the research attribute, on average, 23% of their total sales to direct marketing, with the travel and leisure and retail and wholesale sectors attributing 30%+ of their sales to direct marketing.[2] The uncertainty created by the ECJ decision undercuts confidence in the market for digital trade between the United States and the European Economic Area.

About the DMA Safe Harbor Program

Despite concerns expressed by EU stakeholders around the robust nature of the Safe Harbor Framework, DMA has always taken its role under the Safe Harbor Enforcement Principle seriously. Under the U.S-EU Safe Harbor Framework, U.S. companies interested in self-certification with the U.S. Department of Commerce were required to certify that they adhere to the seven core Safe Harbor principles and FAQs surrounding data collection, protection, choice, security and enforcement. Under this self-certification process, U.S. companies were required to select a third-party dispute resolution provider to serve as a mediator regarding any data privacy complaints that qualify under the Safe Harbor Framework. DMA Members could choose DMA as their Safe Harbor dispute resolution provider. DMA assisted companies with meeting the requirements of the Safe Harbor Enforcement Principle. Under the Enforcement Principle, companies were required to take reasonable steps to ensure that any consumer privacy concern was addressed by: (1) referring consumers to its customer service department or other in-house dispute resolution program; (2) subscribing to a third-party dispute resolution mechanism to address any unresolved in-house consumer data privacy complaints; and (3) having appropriate monitoring, verification, and remedy procedures in place.

As a third-party dispute and enforcement mechanism, DMA members could rely on our decades of experience in addressing and satisfactorily resolving consumer disputes. In addition to dispute resolution, DMA provided technical assistance and educational materials that support member compliance with the Safe Harbor Framework. We actively engaged with the Safe Harbor privacy principles by conducting a staff review of member company privacy policy statements. Members certified under the DMA Safe Harbor program received a DMA Safe Harbor Program mark to display, signifying their alignment with EU principles.

---

[1] Deighton and Johnson, *The Value of Data: Consequences for Insight, Innovation & Efficiency in the U.S. Economy* (2013), *available at* http://thedma.org/valueofdata.

[2] The Direct Marketing Association (UK) Ltd, "Putting a Price on Direct Marketing 2012" (31 July 2012).

Safe Harbor Program participants were required to provide not only company contact information in privacy policy statements, but also the appropriate DMA Safe Harbor contact information. This information promotes clarity, accessibility and transparency within the U.S.-EU Safe Harbor Program.

Under the Safe Harbor self-certification process, American companies must select a third-party dispute resolution provider to serve as a mediator regarding any data privacy complaints that qualify under these frameworks. In this capacity, the DMA Safe Harbor Program currently serves 57 participating member companies, 19 of which enrolled in the last enrollment period alone. In the two years, the DMA has received over 130 complaints through the Safe Harbor complaint process with four qualifying under the Safe Harbor Frameworks. All complaints and inquiries were promptly forwarded to the appropriate contacts and were quickly addressed and resolved.

Our goal is to keep data-driven direct channels open, safe, and productive for business and consumers, helping the DMA to advance and protect responsible data-driven marketing. The Safe Harbor Framework has been integral in allowing the DMA to realize this goal with regard to transatlantic data transfers. DMA and its member companies have long recognized that promoting best practices through effective self-regulation mechanisms like the Safe Harbor Framework enhances consumer trust and confidence. Our members understand that their success in the data driven economy is dependent on consumers' confidence in the online medium, and members support efforts that enrich a user's experience while fostering consumer trust in online channels.

Restoring previously relied upon channels of transatlantic data flow is vitally important to our economy. We thank you for your attention on this important matter. We hope that members of Congress continue to encourage the Department of Commerce to rapidly conclude the Safe Harbor negotiations, and we look forward to continuing to work with you on this important issue.

Respectfully Submitted,

Christopher Oswald
Vice President, Advocacy
Direct Marketing Association

ITIF | INFORMATION TECHNOLOGY & INNOVATION FOUNDATION

Testimony of

Robert D. Atkinson, Ph.D.

Founder and President

The Information Technology and Innovation Foundation

on

"International Data Flows:

Promoting Digital Trade in the 21st Century"

Before the

House Judiciary Committee

Subcommittee on Courts, Intellectual Property, and the Internet

November 3, 2015

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

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

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

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

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

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

Why Data Innovation Is Important

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

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

Why Free Trade in Data Is Important

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Barriers to Digital Trade

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Countries' Motivations for Limiting Free Trade in Data

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Where Are We Now?

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

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

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

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

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

Policy Steps to Enable Digital Free Trade

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Endnotes

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

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

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

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

AMERICAN ACTION
FORUM

Douglas Holtz-Eakin
President, American Action Forum
November 2, 2015

Statement for the House of Representatives Subcommittee on Commerce, Manufacturing, and Trade and the Subcommittee on Communications and Technology Joint Hearing entitled "Examining the EU Safe Harbor Decision and Impacts for Transatlantic Data Flows"[1]

The Safe Harbor program has been a key component of global Internet commerce and has facilitated frictionless transfer of commercial information between the United State and Europe. The European Court of Justice's (ECJ) decision to nullify the arrangement throws digital trade into turmoil. For the over 4,400 U.S. businesses and the millions of jobs that relied on this agreement as a means of moving information, the absence of a data transfer regime will be costly; the Internet could be balkanized and transatlantic digital competition could suffer from being frozen in place.

To ensure this isn't the case, both Congress and the White House should take very seriously the task of reestablishing the free flow of data between to the two regions via a Safe Harbor 2.0. Fortunately, the affected parties have until January 2016 to negotiate a new set of protocols. At the same time, Congress and the Administration should resist demands for broader privacy regulation. Such regulation is at odds with the timetable and misses the reality that U.S. system is more robust and beneficial than it is often perceived to be.

The stakes are high. The ECJ decision affects a trading block that accounts for a third of all world trade and nearly half of global economic output. While it is still in the early phase, the impact could reverberate throughout digital trade, which has been growing steadily. In 2012, the U.S. exported "$140.6 billion worth of digitally deliverable services to the EU and imported $86.3 billion worth," for a total of $227 billion.[2] As a practical matter, U.S. companies might soon have to localize data on European servers and limit transfers of data between the U.S. and the EU, thus fracturing the open Internet. This will also ensure that the biggest players in the tech economy face reduced competition from newcomers since the compliance costs of this new and complicated legal regime will hinder startups.[3]

There are other means to ensure compliance with European laws, including model contract clauses and binding corporate rules, for example. However, a key part of the model contract clauses still

---

[1] The opinions expressed herein are mine alone and do not represent the position of the American Action Forum.

[2] Joshua P. Meltzer, *The Importance of the Internet and Transatlantic Data Flows for U.S. and EU Trade and Investment*, http://www.brookings.edu/~/media/research/files/papers/2014/10/internet-transatlantic-data-flows-meltzer/internet-transatlantic-data-flows-version-2.pdf.

[3] Adam Thierer, *Unintended Consequences of the EU Safe Harbor Ruling*, http://techliberation.com/2015/10/06/unintended-consequenses-of-the-eu-safe-harbor-ruling/.

hasn't been fully recognized for use,[4] while binding corporate rules would take some time to implement across businesses and would be burdensome to small and medium sized companies.[5] Safe Harbor 2.0 should meet the legal needs of both sides of the Atlantic without being burdensome to either side.

There has been progress already. Congress should be lauded for its quick action to pass the Judicial Redress Act to address the Court's concern that aspects of the law compromise "the essence of the fundamental right to effective judicial protection." The Federal Trade Commission (FTC) has worked hand in hand with the European regulators to address "issues such as the FTC's enforcement powers; jurisdiction over employment data; the sectoral exemptions to our jurisdiction; and educating European Union consumers on Safe Harbor."[6] The Department of Commerce should be lauded as well for its quick response to this decision in securing a basic set of working principles on which both sides could agree.[7]

There is danger from overreach as well. Some have used the ECJ decision as a justification to call for broader privacy regulation. Broad privacy regulation is inconsistent with the January 2016 timetable, running the risk of leaving commercial needs unaddressed. But such a call misinterprets what is needed for the next version of Safe Harbor.

The U.S. system does not rely on pure procedures of the type the ECJ highlighted in its decision, a fact that would be revealed by a thorough examination of the privacy practices on the ground.[8] The U.S. privacy policy is characterized by a robust ecosystem of substantive, sectoral protections that allow U.S. companies to compete. As part of getting the balance right between privacy protection and competitive commerce, the FTC has tried a number of cases and secured 20-year consent decrees with some of the largest Internet-based firms, which requires that they submit to independent audits. While the Commission has sustained its fair share of criticism for these actions – ranging from insufficiently concerned with privacy to overly zealous – the overall record is one in

---

[4] Melinda L. McLellan and William W. Hellmuth, *Safe Harbor Is Dead, Long Live Standard Contractual Clauses?*, http://www.dataprivacymonitor.com/enforcement/safe-harbor-is-dead-long-live-standard-contractual-clauses/.

[5] Tanya Forsheit and Melinda L. McLellan, *What Now? What Next? FAQs and Answers Regarding the Safe Harbor Decision*, http://www.dataprivacymonitor.com/enforcement/what-now-what-next-faqs-and-answers-regarding-the-safe-harbor-decision/.

[6] Federal Trade Commission Staff, *Privacy Enforcement and Safe Harbor: Comments of FTC Staff to European Commission Review of the U.S.-EU Safe Harbor Framework*, https://www.ftc.gov/sites/default/files/documents/public_statements/privacy-enforcement-safe-harbor-comments-ftc-staff-european-commission-review-u.s.eu-safe-harbor-framework/131112europeancommissionsafeharbor.pdf.

[7] Natalia Drozdiak, *EU, U.S. Agree in Principle on New Data-Transfer Pact*, http://www.wsj.com/articles/eu-u-s-agree-in-principle-on-data-pact-1445889819.

[8] Kenneth A. Bamberger and Deirdre K. Mulligan, *Privacy on the Books and on the Ground*, http://scholarship.law.berkeley.edu/cgi/viewcontent.cgi?article=2305&context=facpubs.

which commercial activity has been supported at the same time that the FTC has acted proactively (albeit often spurred on by privacy advocates) for privacy protection.

The Internet has been a positive economic and social force because of its openness, which should be a central plank of the discussion moving forward. A failure to recognize what is at stake could put the trade of digital goods at risk. Similarly, a failure to recognize that the U.S. privacy regime has been an important component in developing globally competitive companies could be detrimental to negotiations as well. As with many other areas, negotiations for the new Safe Harbor will need a balanced approach.

November 3, 2015

Chairman Michael C. Burgess
Subcommittee on Commerce, Manufacturing and Trade
Committee on Energy and Commerce
United States House of Representatives
Washington, DC 20515

Chairman Greg Walden
Subcommittee on Communications and Technology
Committee on Energy and Commerce
United States House of Representatives
Washington, DC 20515

Ranking Member Janice Schakowsky
Subcommittee on Commerce, Manufacturing and Trade
Committee on Energy and Commerce
United States House of Representatives
Washington, DC 20515

Ranking Member Anna Eshoo
Subcommittee on Communications and Technology
Committee on Energy and Commerce
United States House of Representatives
Washington, DC 20515

Dear Chairmen Burgess and Walden and Ranking Members Schakowsky and Eshoo:

Thank you for holding a very timely joint hearing entitled "Examining the EU Safe Harbor Decision and Impacts for Transatlantic Data Flows."

Together, the Alliance of Automobile Manufacturers, American Automotive Policy Council, and Association of Global Automakers, represent twenty-three major automobile manufacturers. Our member companies take consumer data privacy very seriously. We recognize that the relationship between our companies and their customers is dependent on trust.

Since 2000, the Safe Harbor Framework has been critical to protecting privacy on both sides of the Atlantic and to supporting economic growth in the United States and the European Union. However, the European Court of Justice's recent ruling invalidating the Framework creates significant uncertainty for both U.S. and EU companies and consumers. The implications are far reaching for all areas of commerce, including the auto sector.

We urge lawmakers to forward a prompt conclusion of a new U.S.-EU Safe Harbor Framework that protects consumers' data privacy while ensuring multinational automakers with operations in both the U.S. and the EU can freely transfer information between and among their respective localities. A new U.S.-EU Framework is an essential mechanism to supporting the economic growth that the auto sector is driving in both the U.S. and EU markets. Indeed, the competitive partnerships of U.S. and European automakers are mutually beneficial to each economy's manufacturing sector.

Our companies are global leaders. Not only does data used to conduct business need to be accessed, but access and use of data regarding each entity and regarding those employed by multinational companies should not be firewalled based on our employees' location and citizenship. Restrictions on access to, and the transfer of, such data would impede our companies' ability to effectively and efficiently manage business operations, implicate our regulatory and reporting obligations, and lead to incongruous results, e.g., preventing company managers from accessing data about their own employees unless they are physically located in that country.

One of the key drivers for the resurgence of the U.S. automotive industry has been our ability to focus on operational efficiencies. The unification of many of our information and communications technology (ICT) organizations is part of that strategy. For example, in order to optimize the IT infrastructure we maintain around the world, we need to be able to store and process data in the most efficient manner. Restrictions on transfers, access and use of data could force multinational automakers to maintain servers in specific markets and de-centralize data processing, unnecessarily increasing the costs to produce vehicles and complicating the ICT management at each company.

Perhaps most important to fostering trust with our consumers, our engineering, manufacturing, and distribution networks, as well as warranty repair providers need to be able to freely share their data to ensure we manufacture the highest quality vehicles possible and quickly address problems when they arise. This demands the ability to harness this collective data into information that benefits all our consumers, not just as a whole, but also on an individual, vehicle, level. Unless that warranty data can be traced back to a specific vehicle, it is not especially useful.

The passage of the Judicial Redress Act (H.R. 1428) by the House of Representatives was a positive step forward in meeting the prerequisites for a new Framework. The final enactment of the Judicial Redress Act will be critical in rebuilding the trust of citizens worldwide in both the U.S. government and U.S. industry and in addressing the misconceptions underlying the European Court of Justice ruling. With the implementation of the Judicial Redress Act, the Umbrella Agreement, and the multiple oversight enhancements to U.S. national security practices, we believe the conditions laid out in the ECJ ruling are met and in some cases exceeded. U.S. and EU automakers strongly support the conclusion of U.S.-EU Safe Harbor Framework that protects consumers' data privacy while avoiding interruptions to U.S. and EU automakers' operations. We appreciate the Committee's attention to this critical issue.

Thank you for your consideration of our views.

Sincerely,

Alliance of Automobile Manufacturers
American Automotive Policy Council
Association of Global Automakers

○