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,
This is a preliminary, unedited transcript. The statements within may be inaccurate, incomplete, or misattributed to the speaker. A link to the final, official transcript will be posted on the Committee’s website as soon as it is available.

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
This is a preliminary, unedited transcript. The statements within may be inaccurate, incomplete, or misattributed to the speaker. A link to the final, official transcript will be posted on the Committee’s website as soon as it is available.

Communications and Technology; Lisa Goldman, Counsel; Tiffany Guarascio, Deputy Staff Director and Chief Health Advisor; Lori Maarbjerg, FCC Detainee; Diana Rudd, Legal Fellow; Ryan Skukowski, Policy Analyst; and Jerry Leverich, Counsel for Communications and Technology.
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 is 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.

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 recognize 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.

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.
This is a preliminary, unedited transcript. The statements within may be inaccurate, incomplete, or misattributed to the speaker. A link to the final, official transcript will be posted on the Committee’s website as soon as it is available.

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.

The Chairman. 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
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.

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.

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

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.

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.

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.

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:]

********** INSERT 1 **********
Mr. Burgess. The chair thanks the gentlelady.

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

********** INSERT 2 **********
This is a preliminary, unedited transcript. The statements within may be inaccurate, incomplete, or misattributed to the speaker. A link to the final, official transcript will be posted on the Committee’s website as soon as it is available.

1 Mr. Burgess. The chair thanks the gentleman.

2 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:]

********** INSERT 3 **********
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
This is a preliminary, unedited transcript. The statements within may be inaccurate, incomplete, or misattributed to the speaker. A link to the final, official transcript will be posted on the Committee’s website as soon as it is available.

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:]

39
This is a preliminary, unedited transcript. The statements within may be inaccurate, incomplete, or misattributed to the speaker. A link to the final, official transcript will be posted on the Committee’s website as soon as it is available.

********** INSERT 4 **********
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. Okay. 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, you know, 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, you know, all forms of, you know, 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. -- 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, you know, 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
This is a preliminary, unedited transcript. The statements within may be inaccurate, incomplete, or misattributed to the speaker. A link to the final, official transcript will be posted on the Committee’s website as soon as it is available.

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. -- that is accessible to them so they can look at data with proper warrants -- 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. -- 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. -- with the scope of the problem.

Mr. Rotenberg. I think we should update our national law. I mean, 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 an interest 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. Okay. 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, you know, 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, you know, 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
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. You know, 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, you know, 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
infrastructure 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
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, you know, 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
This is a preliminary, unedited transcript. The statements within may be inaccurate, incomplete, or misattributed to the speaker. A link to the final, official transcript will be posted on the Committee’s website as soon as it is available.

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 follows:]

********** COMMITTEE INSERT **********
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. -- balance can be found.
Ms. Eshoo. -- 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. -- 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. -- 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. -- post-Snowden --

Ms. Espinel. -- 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, you know, a long-term sustainable --

Mr. Lance. Yes.

Ms. Espinel. -- 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, you know, 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. -- 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 problem 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
This is a preliminary, unedited transcript. The statements within may be inaccurate, incomplete, or misattributed to the speaker. A link to the final, official transcript will be posted on the Committee’s website as soon as it is available.

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. Okay. 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. So, you know, 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.

You know, 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. Okay. 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, you know, 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. Okay. 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.

And, you know, 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,
you know, 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, you know, 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 -- I mean it is just -- 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 okay for them locally within their own cyber -- you know, their 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. -- could be -- 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. What -- 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 international 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, as I was saying, I think -- I would say a couple of things. You know, 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. Okay. 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 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 follows:]

********** COMMITTEE INSERT **********
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
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. -- between U.S. persons and non-U.S. persons.

Mr. Pompeo. Fair enough. Just so know, that would be ahistoric. 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. -- about policy. I am asking about policy and --

Mr. Rotenberg. SF-86, those --

Mr. Pompeo. Yes.

Mr. Rotenberg. -- 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. -- 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, you know, 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. I will not read them unless asked.

[The information follows:]

********** COMMITTEE INSERT **********
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.]