

RPTS BINGHAM

DCMN BURRELL

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

HEARING ON "INTERNET PRIVACY:

THE IMPACT AND BURDEN OF EU

REGULATION"

THURSDAY, SEPTEMBER 15, 2011

House of Representatives,

Subcommittee on Commerce,

Manufacturing and Trade,

Committee on Energy and Commerce,

Washington, D.C.

The subcommittee met, pursuant to call, at 11:20 a.m., in Room 2322, Rayburn House Office Building, Hon. Mary Bono Mack [chairwoman of the subcommittee] presiding.

Present: Representatives Bono Mack, Blackburn, Stearns, Harper, Lance, Olson, McKinley, Pompeo, Kinzinger, and Butterfield.

Staff Present: Charlotte Baker, Press Secretary; Andy Duberstein, Special Assistant to Chairman Upton; Brian McCullough,

Senior Professional Staff Member, CMT; Jeff Mortier, Professional Staff Member; Gib Mullan, Chief Counsel, CMT; Shannon Weinberg, Counsel, CMT; Tom Wilbur, Staff Assistant; Alex Yergin, Legislative Clerk; Michelle Ash, Minority Chief Counsel; Felipe Mendoza, Minority Counsel; and William Wallace, Minority Policy Analyst.

Mrs. Bono Mack. The subcommittee will now come to order. Good morning. Few things today have impacted more people than the Internet. Over the past decade, there has been a huge explosion in the use of the Internet. It has changed the way we work, shop, bank and live. But it has also resulted in a new dangerous contagion of sorts involving piracy threats such as malware, spyware, phishing, pfarming, and a long list of assorted computer cookies. The time has come for Congress to take these growing threats more seriously.

The chair now recognizes herself for an opening statement.

Today, as we continue our series of hearings on Internet privacy, we are going to take a close look at the impact of regulations on commerce, consumers and businesses. As chairman of the subcommittee, I am guided by one critically important question: When it comes to the Internet, how do we balance the need to remain innovative with the need to protect privacy?

As someone who has followed this issue very closely over the years and someone who, frankly, remains skeptical right now of both industry and government, I will continue to keep an open mind as to whether new legislation or regulations are warranted. But let me be clear about one thing. To date, I do not believe industry has proven that it is doing enough to protect American consumers while government, unfortunately, tends to overreach every time it gets involved in the marketplace. From my perspective, there is a sweet spot between too much regulation and no regulation at all. My goal is to find that sweet spot.

Today, the Internet pretty much remains a work in progress, even though it serves billions of users worldwide and while e-commerce in the United States will top \$200 billion this year for the first time, there is still a Wild, Wild West feel to cyberspace, leaving many consumers wondering whether there is a sheriff in town or whether they are completely on their own when it comes to protecting themselves and their families.

In just 25 years, the Internet has spurred sweeping transformative innovations. It has become embedded in our daily lives, and it has unlimited potential to effect positive social and political change. Yet every single day, millions of Americans are subject to privacy threats. Most of them by and large are seemingly innocent, such as the collection of information about consumer buying habits, but some of them are malicious and criminal, often involving online theft and fraud.

This subcommittee has a responsibility and a unique opportunity as well to ferret out those differences and to do everything we can to keep the Internet free while keeping consumers free, to the extent possible, from widespread private abuses.

I for one do not subscribe to the theory that privacy is dead, get over it. There are smart ways to protect consumers and to allow e-commerce to continue to flourish. That is the sweet spot we should be searching for in all of our hearings.

Additionally I will continue to work with Members on both sides of the aisle to secure passage this year of the SAFE Data Act, which

will provide American consumers with important new privacy safeguards.

Today we are taking a close look at the EU's Data Privacy Directive, first adopted on October 24, 1995. The EU model is one of the largest regulatory regimes in the world. I believe this hearing will be instructive, allowing us to better understand some of the lessons learned over the past 15-plus years. Clearly there have been some unintended consequences as a result of the directive which have proven problematic for both consumers and businesses.

The purpose of the directive is to harmonize differing national legislation and data and privacy protections within the EU while preventing the flow of personal information to countries that, in the opinion of EU regulators, lack sufficient privacy protections. But as we will learn today, there has been no shortage of unintended consequences. In a way you could say that the EU directive at some point crossed paths with Murphy's law -- anything that can possibly go wrong, does.

Unfortunately, in all too many cases it has gone wrong for American businesses trying to navigate these tricky regulations. The directive requires all EU member states to enact national privacy legislation which satisfies certain baseline privacy principles ranging from notice, to consent, to disclosure, to security. And while these principles are the basis for the directive, each EU member state is responsible for incorporating these articles into its own national privacy laws. This in turn has led to inconsistent regulatory regimes throughout the EU and has created serious problems for American

multinational firms.

Making matters worse, compliance within the EU remains fractured, with several member states not fully complying with the directive. This has led to sporadic and inconsistent enforcement, with a seemingly disproportionate number of American companies targeted for compliance violations.

Let me be clear. My purpose in holding this hearing is not to point fingers. Instead, my goal is to point to a better way to promote privacy online and to promote e-commerce. In the end this will benefit both American consumers and American businesses and send a strongly held belief all across America that the Internet should remain free.

And with that, the gentleman from North Carolina, Mr. Butterfield, the ranking member on the Subcommittee on Commerce, Manufacturing and Trade, is now recognized for 5 minutes for his opening statement.

Mr. Butterfield. Thank you, Chairman Bono Mack. Thank you for holding today's hearing on the European Union's efforts to protect consumer data. And I especially want to thank the witnesses from the two panels, starting with the Assistant Secretary and the four witnesses on Panel 2. Thank you very much for your testimony today.

The genesis of EU-wide data protection regulation is the Data Protection Directive. And the directive requires the enactment of several principles into the laws of each EU member country. Those principles included granting people access to their personal information, disclosure of which actors are collecting personal data,

affirmative consent prior to personal data being shared with a third party and personal data held by an actor be protected through reasonable security safeguards among other things. This directive along with the subsequent e-privacy directive have provided broad and strong privacy protections for citizens of the European Union member countries.

I commend the EU for recognizing the need to provide baseline privacy policies. Nonetheless, the EU is essentially an association of 27 countries. The point of any EU directive is to standardize the laws of all member countries so they can function as one economic market. The point is not to burden business. It is just the opposite. It is to create a unified and smooth running market across Europe by bringing the laws of each member country closer together.

But enactment, administration and enforcement of those laws remain the responsibility of each individual country. For business that have to navigate the laws of these 27 different countries, some regulations can feel pointless, some paperwork and record keeping burdensome, and some enforcement actions unfair.

I am hopeful that this hearing this morning which reviews the European model will explore both the negatives and the positives of that system. Studying the privacy regimes of other countries can provide valuable lessons for us. Then we must come together to develop a national privacy policy that both protects consumers while promoting economic growth and innovation. That is why it is imperative that we work in a bipartisan fashion to make that happen.

Madam Chairman, I am confident that we can and will do this

together.

I know that this hearing is the second of a series that we will have regarding privacy. I look forward to continuing this important conversation, so we can move forward on crafting a long overdue and well-considered national private policy.

Again, thank you to the witnesses. Thank you, Madam Chairman. I yield back.

Mrs. Bono Mack. I thank the gentleman.

And under the rules of the committee Chairman Upton has yielded his 5 minutes to me, and at this time I would like to yield 1-1/2 minutes to the gentleman from Texas, Mr. Olson, for his opening statement.

Mr. Olson. I thank the chairman for holding another important hearing on Internet privacy. America and Europe have very differing viewpoints toward the protection of personal data on the Internet. Our friends in the European Union believe that privacy is a fundamental human right and that government should be tasked with protecting and regulating personal data. By contrast, the U.S. approach to privacy is a sector-by-sector combination of legislation and industry self-regulation.

These favor a more balanced approach, recognizing personal use of data and sharing while maintaining reasonable safeguards to prevent abuses. With millions of Americans out of work and our economy struggling, the last thing we need to do is to look toward Europe for guidance for new privacy regulations. Instead, we should use today's hearing to look at how the EU's overburdensome privacy laws have

negatively affected the European Union economy and how we can avoid similar pitfalls here at home as we continue to explore whether privacy legislation is needed in Congress.

I thank the chairman. I yield back the balance of my time.

Mrs. Bono Mack. I thank the gentleman and seeing there are no other members present to make an opening statement, we will move to the panels. So we do have two panels of witnesses today joining us. On our first panel we have the Honorable Nicole Lamb-Hale, Assistant Secretary for the International Trade Administration.

Assistant Secretary Lamb-Hale, good morning. Again, thank you very much for coming. You will be recognized for 5 minutes, and to help you keep track of time there are lights and timers. And as you will suspect, the yellow light means either hurry up and hit the gas or slam on the brakes. But either way, you may begin your statement for 5 minutes. Thank you.

**STATEMENT OF THE HON. NICOLE Y. LAMB-HALE, ASSISTANT SECRETARY FOR
MANUFACTURING AND SERVICES, U.S. DEPARTMENT OF COMMERCE, INTERNATIONAL
TRADE ADMINISTRATION**

Ms. Lamb-Hale. Madam Chair Bono Mack, Ranking Member Butterfield, and distinguished committee members, thank you for the opportunity to testify about online privacy and the impact the European Union's legal framework for data protection has on U.S. companies doing business in one or more of the EU member states.

In my capacity as Assistant Secretary for Manufacturing and Services in the International Trade Administration, I will outline the approaches taken by the EU and the United States with respect to commercial data protection, describe the impact that the EU framework has on U.S. companies and explain what the U.S. Department of Commerce is doing to facilitate unencumbered transatlantic trade.

The EU and the U.S. share common goals in desiring to protect individuals' privacy while pursuing economic growth to increase trade and investment and by supporting Internet innovation. The EU directive on the protection of individuals regarding the processing of personal data and the free movement of such data was issued by the European Parliament and the EU Council in 1995 and is currently under review.

The EU directive functions as a baseline for EU member states and allows them to adopt more stringent national protections. In the U.S.,

the protection of individual privacy is deeply embedded in law and policy.

In addition, voluntary multi-stakeholder policy development complements this framework. This framework has encouraged innovation and provided many effective privacy protections. But certain key American players in the Internet, including online advertisers, cloud computing service providers, providers of location-based services and social networking sites, operate in sectors without specific statutory obligations to protect information about individuals. Because of this, the Obama administration is advocating for stronger consumer protection in the online environment.

In the international context, the EU directive imposes limitation on cross border data flows to countries whose legal frameworks do not meet the adequacy requirements of the directive as determined by the European Commission, or the EC, which is the executive arm of the EU.

In 1998, the Department embarked on a 2-year negotiation with EC aimed at devising ways for U.S. companies to continue doing business with firms in the EU without unnecessarily burdensome obligations being imposed on their activities. The result was the U.S.-EU Safe Harbor Framework, which the EC deemed adequate in a July 26, 2000 finding.

The framework remains in force today and is administered by the International Trade Administration on behalf of the United States. It is a voluntary arrangement that allows U.S. commercial entities to comply with the framework principles and publicly declare that they will do so.

When the Safe Harbor Framework was launched, four companies self-certified their compliance to the program. Today nearly 3,000 companies of all sizes belong and more than 60 new members are added each month. This service has enabled small and medium size enterprises to provide a range of value added products and services to EU clients and citizens without the expense of hiring European legal counsel to comply with the EU's legal framework. An estimated half trillion dollars in transatlantic trade is facilitated by the Safe Harbor Framework.

Some large U.S. multinational corporations have chosen alternative means of complying with the directive, but these have proven to be costly and time consuming.

For example, large U.S.-based multinational corporations have chosen to use binding corporate rules, or BCRs, which permit global intracorporate data if the corporation's practices for collecting, using and protecting that data are approved by the data protection authorities in the EU.

Despite recent efforts to streamline the approval process, the cost and time associated with obtaining approval of BCRs are substantial. While the Safe Harbor Framework has proved itself to be valuable in facilitating transatlantic trade, it is not a perfect solution for all U.S. entities. Sectors not regulated by the FTC, such as financial services, telecommunications and insurance, are not covered by the framework because their regulators were not part of the negotiations.

Generally speaking, the biggest problems U.S. companies face with regard to navigating the privacy landscape in Europe include, one, the significant resources that must be allocated to comply with these regulations that they are not in the Safe Harbor; two, several EU member states implement the EU directive differently so U.S. firms must comply with a variety of requirements in as many as 27 member states, and; three, different EU member state regulations create legal uncertainty which complicate U.S. companies' efforts to plan for the future.

The Department continues to engage with the EU and its member states in discussions on how we can allow unimpeded data flows while at the same time respect each other's laws and values. The Department has been engaged in extensive conversation with EU data protection officials at all levels during the more than 10 years since the EU directive entered into force. These interactions have been designed to convey to the EU that the U.S. legal framework, while structured differently, is as robust as the EU's framework for protecting individuals' privacy.

Thank you for the opportunity to explain how the EU's privacy and data privacy framework relates to the commercial interests of the U.S. and to explain what the Department of Commerce is doing to help U.S. companies navigate the regulations in the EU.

I look forward to any questions you may have.

[The prepared statement of Ms. Lamb-Hale follows:]

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

Mrs. Bono Mack. Thank you very much, Dr. Lamb-Hale, for your statement as well as for your insight into the issue of Internet privacy. And I would like to now recognize myself for the first 5 minutes of questions.

And you testified that our current approach to privacy has encouraged innovation and provided many effective privacy protections. Conversely, a number of studies have suggested that EU's approach has actually stifled its Internet economy. Why should we move toward a regulatory approach that has proved to hold back the Internet sector in that particular region?

Ms. Lamb-Hale. Well, certainly we should not work towards an approach that is exactly like the EU's approach. I think it is important to recognize that we need to have a regime that really is flexible enough to take into account changes in technology advancement. The privacy framework that we have in the United States is really about 40 years old, and it doesn't really take into account from a general standpoint principles that can be readily applied to changing technology. And so what we need to do, I think, is to look at the EU example and really work to develop a baseline privacy policy that really provides principles that, again, are flexible, that don't supersede or override existing privacy policy frameworks that are sector by sector, so that we can facilitate trade and we are in a better position to ensure that as we negotiate with our allies and trading partners around the world that we have a basic framework to work from.

Mrs. Bono Mack. Well, in what ways are Europe's complex privacy

regimes discouraging U.S. companies from entering European markets or affecting their success in those markets and do those privacy rules amount to a type of trade barrier?

Ms. Lamb-Hale. Certainly, I want to talk a little bit about our Safe Harbor program which has helped companies in the U.S., almost 30,000 of them, to successfully navigate the EU directive by, quite frankly, allowing them to avoid having to obtain approval from individual data protection authorities and through the Safe Harbor Framework engage in the free flow of information across various countries.

So I think that it is important to look at that as a tool that is something that I think has worked very effectively for our companies, and as we look at what we can do in the U.S. in terms of basic privacy principles, we really need to be sure that we are flexible in our approach, that we aren't looking to promote certain technological innovations, that we really look at principles that can be malleable, quite frankly, so that we can ensure that as new applications come on board like mobile applications that are not covered by our privacy laws that we are able to address those and protect our consumers here and really help to promote international trade with our U.S. companies.

Mrs. Bono Mack. Thank you. Professor Swire will testify in the next panel that the Safe Harbor, which worked well for many years enabling cross border information flow, is not recognized by a number of countries that have adopted privacy regimes in recent years; for example, India, Latin America, Japan, South Korea. Is the ITA working

with these countries to have a Safe Harbor recognized or to ensure its permanence should the EU update a directive? And if so, what has been the reaction of your foreign counterparts?

Ms. Lamb-Hale. Well, certainly, the U.S. Government is engaged in multiple discussions with trading partners around the world, including during the APEC conference that is going on now, looking at how we can work together with our trading partners to come up with a regime that really facilitates international trade and does not impede it.

The Safe Harbor -- companies who take advantage of the Safe Harbor rule or regime are able to take advantage of what are called onward transfer principles, which allow them to contract with European companies and then instead of just being restricted to transferring privacy data between the EU countries and the U.S. to also transfer that data to other countries.

People who take advantage of the onward transfer principles under the Safe Harbor do have that advantage. They do have to meet certain requirements, and the Department is certainly happy to help companies understand those principles so they can take advantage of them in other countries beyond the EU framework.

Mrs. Bono Mack. Thank you very much. I am going to yield back my remaining time, and I now recognize the gentleman from North Carolina for 5 minutes for his questions.

Mr. Butterfield. Thank you, Madam Chairman. Let me begin with this, and again, thank you very much for coming in and thank you for

your testimony and, more importantly, thank you for your service to the Department and to the country.

One issue we are exploring is how privacy legislation would affect U.S. firms globally. We have heard from some multinational companies that baseline privacy protections in the U.S. would help them abroad. In your testimony you mentioned the Commerce Department has received comments from industry who say that an enhanced U.S. privacy framework could reduce barriers and compliance costs for U.S. companies in international markets.

Can you briefly describe some of these comments and discuss whether you agree that U.S. firms could see a benefit abroad if we enacted legislation here?

Ms. Lamb-Hale. Yes. Thank you very much, Mr. Butterfield.

It is important as we look at our global competitiveness that we have a framework, a set of basic principles that can be found in one place, that really speak to the value that the United States places on privacy protection. We certainly place a lot of value on that, and I think that the world knows that. But in order to really discover our principles you have to parse through a number of different pieces of legislation by sector to really get the sense of what the privacy protection regime is like in the United States.

And so as a result as we enter into negotiations with our trading partners, it would be helpful, and I think it would help the competitiveness of our businesses, if we had baseline consumer privacy protections, principles that are flexible and that take into account

really the changing economy, the changing technologies, so that when we go in we don't have to have a situation where our service providers who are engaging in trade with the EU and with other countries are impeded because those countries are concerned about our data privacy regime.

Mr. Butterfield. So you are saying that this baseline legislation could address or alleviate some of the concerns that EU countries have raised regarding our firms?

Ms. Lamb-Hale. I think so. I think so, Mr. Butterfield. I mean certainly through the Safe Harbor Framework we have been able to help our businesses navigate very successfully the EU directive. But I think going forward and as we look at our negotiations with multiple countries, including through our APEC negotiations and our work with the OECD and others, I think it is important that if we have our privacy principles in one place, just as the EU does, quite frankly, through their directive, if we have one document as opposed to multiple documents that you have to parse through to really get the sense of what our basic principles are, I think that our companies will be more competitive globally.

Mr. Butterfield. Well, let me ask you to speak to your agency specifically. Would a baseline EU privacy law help your agency as it negotiates with non-European countries?

For example, we have heard fears that some Asian countries are looking to the EU as they draft their first privacy laws. Would having a U.S. law in place change that dynamic in any way?

Ms. Lamb-Hale. I think so. I think that often around the world because the EU directive is in a single document, so to speak, that people look to that as the standard. And I think that certainly as we have seen, there are some difficulties with the implementation of that directive. It really increases the compliance cost of our companies as they trade with the EU countries. And so I think to have another model to use in our negotiations around the world that really could demonstrate the U.S.'s leadership in this regard would be very helpful to the global competitiveness of our companies.

Mr. Butterfield. Thank you. Finally, in your testimony, you state that U.S. companies face three major problems with regard to navigating the EU privacy landscape. The first one on your list is the significant resources that must be allocated to comply with these regulations. I understand that companies that aren't regulated by the FTC aren't eligible for the Safe Harbor. This universe includes financial services, telecommunications and insurance companies.

Help me with that. I don't fully understand it. Can you clarify for me, are these companies you refer to as not in the Safe Harbor and that have to allocate significant resources to comply?

Ms. Lamb-Hale. Yes. As was mentioned earlier, the Safe Harbor is only applicable to companies that are regulated by the FTC and also the Department of Transportation. And so to the extent that companies are not regulated by those entities, they have to look to other methods, including in some cases binding corporate rules that they institute that only apply to intracompany transfers of data.

And so to the extent that we have a baseline set of principles that would apply across the board that would not supersede existing regulatory frameworks that would cover financial services and other sectors, but if we have a set of baseline principles, I think that it will reduce the compliance costs, quite frankly, of our companies around the world as they do business, and it is something that we should certainly consider. The Obama administration is very supportive of it. We have certainly through our green paper and we are working on a white paper that sets forth the framework that we think would be helpful to protect both U.S. companies and our citizens.

I think that as we look to that, it will really help our companies to be competitive globally.

Mr. Butterfield. Thank you. I yield back.

Mrs. Bono Mack. I thank the gentleman.

The chair now recognizes Mr. Olson for 5 minutes.

Mr. Olson. I thank the chair and I want to thank the Assistant Secretary for coming today to give your time and your expertise. Welcome.

Ms. Lamb-Hale. Thank you.

Mr. Olson. I have a couple of questions for you, ma'am.

According to the Interactive Advertising Bureau advertisement revenues in the United States hit \$7.3 billion for the first quarter of 2011, a 23 percent increase, 23 percent over the same period last year. Further, ad revenues increased from under \$1 billion in 1999 to its current total of \$7 billion.

Do you think this type of economic growth could be achieved if the U.S. were operating under a EU type privacy regime?

Ms. Lamb-Hale. No. And we are certainly not advocating that the U.S. operate under that kind of a regime. I think the issue with the EU privacy regime is that it is applied inconsistently across the U.S. or the EU member states, the 27 member states. And the goal would be not to do that in the United States. The goal would be to come up with basic principles that include input from the multiple stakeholders that are concerned about these issues and to develop something that is applied uniformly and, quite frankly, does not supersede existing regimes. We are really, our effort is to plug gaps, gaps that exist in the privacy regime that quite frankly could not be anticipated at the time that those various laws were enacted because, of course, we have had innovation through the Internet and generally in the economy.

So the goal is to have a set of principles that are basic principles that, quite frankly, can then be used to assist in the development of further innovation and protect our citizens and create competitiveness for our companies around the world.

Mr. Olson. Thank you. And switching gears a little bit just talking about the Safe Harbor issue, the FTC recently brought its first case alleging that a company did not satisfy the requirements of the U.S.-EU Safe Harbor. The Safe Harbor is supposed to help U.S. companies compete in Europe, not let the European Parliament write our laws for us. What is this administration doing to make sure that Safe Harbor is protecting U.S. companies?

Ms. Lamb-Hale. Well, we certainly work with our U.S. companies who are a part of the Safe Harbor very closely when they have situations within the EU where there are alleged violations. We certainly work in a low key fashion because often the companies don't want a lot of publicity in this regard. So we really do it on a case-by-case basis.

We feel that the services that we provide companies, the education that we provide about the ins and outs of the Safe Harbor are helpful to them and we work with them as they come to us with situations that they have faced in the EU notwithstanding the Safe Harbor Framework.

Mr. Olson. One final question for you, Assistant Secretary. Has the administration performed any type of compliance cost analysis for the privacy directive, and if not, do you plan to do so?

Ms. Lamb-Hale. Yes, we do have some general information on compliance costs. And I can say to you that it is certainly more expensive not to comply than it is to comply. And so what we encourage our companies to do is to be engaged and be educated about the various regimes. To the extent that they are in the Safe Harbor I think they have a leg up because they are able to operate without having to obtain approval from various data protection authorities around the EU.

But we certainly work with the companies to ensure that they are educated and that we have their costs -- while there will always be costs associated with operating in other countries and in the EU, but their costs are limited.

Mr. Olson. Thank you for those answers. I yield back the balance of my time.

Mrs. Bono Mack. I thank the gentleman and now recognize the gentleman from West Virginia for 5 minutes, Mr. McKinley. And he waives. So next we will go to Mr. Harper for 5 minutes.

Mr. Harper. I will waive.

Mrs. Bono Mack. And he waives.

Mr. Stearns for 5 minutes. Mr. Stearns.

Mr. Stearns. Thank you, Madam Secretary. How are you?

Ms. Lamb-Hale. I am fine, thank you.

Mr. Stearns. I think one thing that a lot of us are concerned about is that the EU has set up these privacy laws as sort of a subterfuge to provide anti-competitive protection for the EU, to sort of favor their own businesses.

Do you sense any sense of that, not overtly but covertly, that some of these foreign countries because the U.S. lacks a formal privacy law, is using this as a way to protect they themselves?

Ms. Lamb-Hale. Well, Mr. Stearns, I don't want to speculate on the intent of the EU in their directive.

Mr. Stearns. Well, maybe instead of speculate, have you found that it has sort of been true?

Ms. Lamb-Hale. I don't know that it is true. I think that certainly the problem and the lesson to be learned from the EU experience is that having individual member states create their own regimes and as they interpret the requirements of the directives has increased costs for our companies. It has created regulatory uncertainty for our companies who are doing trade with the EU.

So certainly our goal is to work very closely with the EU. We have done it over the 10 years since the Safe Harbor was put in place, to really work together to come up with an approach that really helps both of our interests.

Mr. Stearns. Do you have any idea what the costs, economic impact, any studies that show the dollars that it would cost Americans more? I think we have here studies that show the economic impact to U.S. companies if such regulations at the EU are implemented what it would cost American companies. Do you have any studies like that?

Ms. Lamb-Hale. What I can tell you, sir, that our findings, there are findings that have indicated that the average compliance costs were \$3.5 million but the costs for noncompliance were nearly three times higher at \$9.4 million. And so certainly noncompliance is more expensive.

Mr. Stearns. Because if they don't comply, their market is shut down is what you are saying?

Ms. Lamb-Hale. Well, I would imagine in the various member states there are penalties that are I would imagine would need to be paid. There are costs to deal with the, whatever the allegations would be in terms of not complying, noncompliance with the EU directive as interpreted by the individual member states.

So I don't have an exact number that I could give you per year. But I can tell you this, that we do see that there are significant compliance costs. It does, it has impacted trade, but because of our kind of knowing that back in 2000, when the directive was really, when

the Safe Harbor Framework was accepted by the EC as being adequate and 30,000 of our companies now today are part of that framework, it has helped those companies to navigate some of these costs.

Mr. Stearns. When I pick up a magazine and I look at the ads and I give it to my son or I give it to other family, they all see the same ads. But in the United States if I pick up, if I go on the Washington Post Web site, they are often behavioral because they have maybe a record of things about me, they have some behavioral advertising. They can really selectively decide when I pull up the Washington Post that these ads would be more interesting to me. So that the advertisers have an incentive to have this behavioral advertising. But it is not true in the European Union, is that correct?

Ms. Lamb-Hale. Well, the --

Mr. Stearns. In other words, the behavioral advertising that we allow our companies to selectively accumulate, the Googles, the Amazon dot-coms, books and things like Barnes and Noble, all of that goes into the mix and gives a behavioral opportunity for advertisers to narrow down who they are going to advertise. But you can't do it that in the European Union, is that correct?

Ms. Lamb-Hale. Well, I can't speak to the various states --

Mr. Stearns. If you don't know, just say yes or no.

Ms. Lamb-Hale. I don't know the answer with respect to the various states because all of the various states have their own national laws that interpret the requirements under the directives.

Mr. Stearns. As I understand, the majority of the EU states, the

27 of them, you have to opt in to get this behavioral advertising? Do you know if that is true?

Ms. Lamb-Hale. I don't know the answer to that. I can certainly get back to you.

[The information follows:]

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

Mr. Stearns. That would be interesting to the chairlady and to others to see the 27 States, what they do.

Now, who is the controlling authority in the European Union, or does the data privacy agency of each of the 27 function independently of the EU? There is no FTC.

Ms. Lamb-Hale. There is a European Commission, which is the entity that has the overarching authority --

Mr. Stearns. Is that equivalent to the FTC?

Ms. Lamb-Hale. Roughly. I guess that would be a good analogy to draw.

Mr. Stearns. But you also indicated that each of the 27 countries do their own thing and so it doesn't seem to be --

Ms. Lamb-Hale. And that is the problem, that is the lessons learned.

Mr. Stearns. A European preemption here, they can't preempt these other 27?

Ms. Lamb-Hale. Well, it is certain there is a baseline that is established by the directive, and each of the member states can then enact their own laws. And that is where some of the problem comes in and that is a lesson to be learned. That is something that we wouldn't want to have in the United States.

Mr. Stearns. Thank you.

Mrs. Bono Mack. And the gentleman's time has expired, and the chair now recognizes Mr. Pompeo for 5 minutes.

Mr. Pompeo. Thank you, Madam Chair. Do you have any data, Madam

Secretary, on how the costs and benefits you describe impact different businesses; that is, small business or larger U.S.-based businesses or U.S.-based multinational business? Do you have any data that suggest how those costs and benefits fall for those different types of businesses?

Ms. Lamb-Hale. I don't have specific data for you. I can tell you that we have found that for companies that don't participate in the Safe Harbor, there are significant costs associated with that. The Safe Harbor is a wonderful program because really it is very cost effective once you establish the -- show that you have satisfied the requirements to join, it is a \$200 initial fee and \$100 to maintain it each year. Companies who don't take advantage of that, both large and small, do have more significant costs.

We can certainly get some information to you though to kind of break it down by company size if we have that.

[The information follows:]

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

Mr. Pompeo. Thank you very much. Madam Chair, I yield back my time.

Mrs. Bono Mack. I thank the gentleman. And seeing no other members present, I again want to thank the Secretary very much for being with us today. You have been very gracious with your time. I look forward to working with you on this in the future and going forward. And again it has been a very insightful discussion and thank you for your time.

Ms. Lamb-Hale. Thank you, Madam Chair.

Mrs. Bono Mack. Now we will quickly move into the second panel. If the second panel could begin taking their seats we would like to move along as quickly as possible in hopes of not having to run into a series of votes on the floor.

Thank you all very much. So we have four witnesses joining us today in the second panel, our first which is Catherine Tucker, Douglas Drane Career Development Professor in IT and Management and Associate Professor of Marketing at MIT Sloan School of Management. Our second witness is Stuart Pratt, President, Consumer Data Industry Association. Our third witness is Paula Bruening, Deputy Executive Director and Senior Policy Adviser at the Centre for Information Policy Leadership. And the final witness this morning is Peter Swire, Professor of Law at Moritz College of Law at the Ohio State University.

Good morning, still, everyone and thank you very much for coming. You will each be recognized for 5 minutes, as you know, and I think you know how the lights work. Make sure you remember to turn the

microphone on before you begin. And I would like to begin with Ms. Tucker for 5 minutes -- Dr. Tucker -- excuse me -- for 5 minutes.

STATEMENTS OF DR. CATHERINE TUCKER, DOUGLAS DRANE CAREER DEVELOPMENT PROFESSOR IN IT AND MANAGEMENT AND ASSOCIATE PROFESSOR OF MARKETING, MIT SLOAN SCHOOL OF MANAGEMENT; STUART PRATT, PRESIDENT, CONSUMER DATA INDUSTRY ASSOCIATION; PAULA J. BRUENING, VICE PRESIDENT, GLOBAL POLICY, THE CENTRE FOR INFORMATION POLICY LEADERSHIP, HUNTON & WILLIAMS, LLP; AND PETER P. SWIRE, C. WILLIAM O'NEILL PROFESSOR IN LAW AND JUDICIAL ADMINISTRATION, MORITZ COLLEGE OF LAW, THE OHIO STATE UNIVERSITY

STATEMENT OF DR. CATHERINE TUCKER

Ms. Tucker. Good morning. I want to thank the committee for inviting me to speak. I was truly honored. My testimony is going to describe research I have done into how European privacy regulation has affected the performance of online advertising.

Now, the motivation behind this research is you may have many good reasons to want to protect consumer privacy online, we also may have many reasons to want to harmonize with our European trading partners. However, there is a risk that strict regulations can damage the ability of Internet firms that support it through advertising and the advertising industry can tend to be hurt. Why is this? It is because the business model for nonsearch advertising online is really based around the usage of data. And so an example of that is say I am a Cadillac dealer, it means that I can only, I can choose to just show ads to people who have been recently searching car review Web sites. And this means I save money because I am not actually showing ads to people who are not going to be in the market for a car.

So therefore understanding how limiting data can hurt advertisers, I think it makes sense to try and understand what is happening in the EU.

So in my paper, I actually examined the effect of the European Privacy and Electronics Communications Directive of 2002, sometimes known as the e-Privacy Directive. And what this e-Privacy Directive

did was it clarified how the more general principles of 1995 were applied to the Internet and communications sector.

Now several provisions of this e-Privacy Directive limited the ability of companies to track user behavior online and then use the data for the kind of behavioral targeting that was inherent in my Cadillac dealership example.

The data I used in my study was collected by a marketing research company over a decade and it is based around the gold standard of social science research, which is a randomized trial, much like used in medicine where some people see an ad and some people do not, and to compare how the ad performance implied by these randomized trials changed in Europe relative to the rest of the world after the implementation of the e-Privacy Directive.

This is a large scale study. I used data from 3.3 million consumers and over 10,000 online advertising campaigns.

The first key finding is that the e-Privacy Directive was associated with a 65 percent decrease in online advertising performance, the advertisers that I studied. This is a sizeable decrease, and I think the best way of understanding it is that if an ad is not targeted appropriately, consumers online are really very good at ignoring it.

Now I think this is coming up in the questioning earlier, what does this 65 percent mean in real terms for American businesses? Well, the public policy group NetChoice took the estimates of my study to project that EU star regulation could cost U.S. businesses \$33 billion

over the next 5 years. So this is obviously a large negative effect.

But I also want to emphasize the second set of findings. And this was how the regulation affected different ads differently. And what I saw was that ads on Web sites that had content that is not easily matched to a product category, think of a news Web site, think of an Internet service site such as dictionary.COM, ads on those Web sites, they were the ones that were really hurt. And why is that? Well, you really need external data in order to target advertising. On the other hand ads on travel Web sites, baby Web sites, they kept on working as well before and after regulation because you are just going to keep on advertising diapers and hotels on these types of Web sites.

The other kinds of ads that were really affected were small and unobtrusive banner ads, the kind of ads that I would describe as being annoying, the ones that float over your Web site when you are trying to read it, those weren't affected. It was really the ads that were designed to be informative. And so I think this leads to a second set of concerns which means that privacy regulation can lead to a set of incentives which means that advertisers switch to more intrusive and annoying advertising because they can't actually target ads in a relevant way, and also that Web site developers might switch to more commercial shall we say content in order to target advertising by means of the category.

So thank you, and I look forward very much to your questions.

[The prepared statement of Ms. Tucker follows:]

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

Mrs. Bono Mack. Thank you very much, Dr. Tucker.

Mr. Pratt, you are now recognized for 5 minutes.

STATEMENT OF STUART K. PRATT

Mr. Pratt. Chairwoman Bono Mack and Ranking Member Butterfield and members of the committee, thank you for this opportunity to testify. I am going to work through a few key points. Obviously you have the written testimony for the record. And first and most importantly, we must preserve what is best about the U.S. marketplace for data flows that we have today.

CDIA members' data and technologies protect consumers and they help U.S. businesses to manage risks and empower economic opportunity. Whether it is counter-terrorism efforts, locating a child who has been kidnapped, preventing a violent criminal from taking a job with access to children or the elderly or ensuring the safety and soundness of lending decisions, our members' innovative databases, software and the analytical tools are critical to how we manage risk in this country and ensure fairness and, most importantly, how we protect consumers.

The U.S. has a long and successful track record of protecting consumers and fostering commerce at the same time. I think it is an important balance that we have to continue to maintain as we go forward. And, in fact, the United States is really at the forefront of establishing sector specific enforceable laws regulating uses of personal information of many types, and the list is extensive and

includes for example the Fair Credit Reporting Act, the Gramm-Leach-Bliley Act, the Health Insurance Portability and Accountability Act, the Drivers Privacy Protection Act, and many more. CDIA believes this sector-by-sector approach has not just worked well but has ensured that the United States has both a marketplace that puts consumers first and one that is the most robust, innovative and efficient.

CDIA's members, however, are global companies and they do understand the importance of international engagement and dialogue. Our members are the most successful companies in the world when it comes to producing data that protects consumers and allows for effective risk management which facilitates competition. Historical experiences, cultural mores and much more drive the individual countries' deliberations about how to protect their citizens' data, and this is no less true for us here in the United States. Our members respect these differences. We engage in regional discussions with organizations such as the Asia Pacific Economic Cooperation and the European Union.

Our members have successfully encouraged countries to adopt practices that have made the U.S. successful. Just look at the last 18 months, for example. Both Brazil and Australia have shifted their laws to permit the development of full file credit recording systems which will inure benefits to their citizens much as the U.S. credit reporting industry has done for the last 100 years. This type of constructive engagement will continue. It is likely the best approach

to managing global data flows even as we choose different approaches to how we may regulate data flows domestically.

We must protect our domestic success and weigh consequences carefully. Like every other global commerce issue, there is no dearth of opinion about how consumer data should be used and protected. Because of this one cannot turn to Europe with the assumption that their work is a reflection of world opinion.

There have been many different approaches to establishing basic principles for the protection of data, and we list a number of examples in our written testimony. Even in Europe the Data Protection Directive has been transposed into country specific laws which while determined as adequate by the European Union are still different.

A real world example of how this affects commerce can be drawn from the credit reporting industry. The credit reporting industry in Europe is balkanized. It impinges on data flows across countries. It has impinged on the ability for Europe to develop a true continental financial services marketplace where banks in Germany would compete with banks in France, for example.

So the EU is a less than perfect solution in many different ways.

It isn't new news that Europe and the U.S. differ when it comes to data protection. Even our fundamental system of enforcement for consumer protection differs. It is our view that bringing a European Union style law to the U.S. would result in significant increases in private litigation, something that Europe doesn't face but which we have as a tradition in this country. It is one of the reasons why we

take it so seriously when somebody says we should look to Europe, for example, for the type of structure that we should have here in the U.S.

We have privately enforced laws. We have a tort system that encourages private enforcement by individual consumers and through class actions. That does not exist in Europe and that is a radical difference between how Europe and its legal regimes work and how ours work here in the United States.

It is our view that the U.S. model has worked exceptionally well for our citizens and for our economy. We continue to support international engagement, regional data flow agreements, but also the preservation of our U.S. sector specific approach to law because laws resulting from this approach are far more likely to respect free speech rights in our Constitution. Laws are more likely to be focused and not overreaching in a manner that would impinge on innovation.

Laws are subject to the deliberations and oversight of Congress, which is obligated to represent the interests of citizens of this country and because decisions about data protection will not be an abrogation of congressional authority through the establishment of a new Federal regulator with regulatory powers that overshadow the legislative authority of the Congress itself. History has proven that our approach works well.

I thank you for this opportunity to testify, and I am happy to answer your questions.

[The prepared statement of Mr. Pratt follows:]

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

Mrs. Bono Mack. Thank you very much, Mr. Pratt.

And Ms. Bruening, you are now recognized for 5 minutes.

STATEMENT OF PAULA J. BRUENING

Ms. Bruening. Thank you, Chairman Bono Mack, Ranking Member Butterfield, members of the committee. Thank you for the opportunity to testify today about the EU directive.

Privacy and protection of data are values shared by the United States and our friends in Europe. Both the EU and U.S. guidance about the responsible collection, use, storage and sharing of information about individuals is based on trusted, relevant, long-established principles of fair information practices.

But the European directive enacted in 1995 has challenged in many respects the rapid rate of technological change, the emergence of new business models, and the exponential growth of the rate in which data is generated and shared around the world.

This dynamic marketplace requires a responsible yet flexible approach to data protection. Instead, the directive imposes administrative notification requirements on companies that often do little to advance privacy protections but that place significant burdens on companies.

It obligates persons responsible for data to notify EU member state data protection authorities of the processing of personal data. Such notification is required when information systems are created and

modified and when personal data is transferred outside the European Union.

It requires companies transferring personal data to countries outside the EU not considered to have adequate data protection to notify the data protection authorities of the member states of the transfer and in some cases obtain a prior approval. Such approval can take easily 6 months to obtain and at the cost of significant resources for the company and the data protection authorities.

This lack of harmonization between 27 member states adds to this burden, as each may impose requirements that differ to some extent from others, sometimes in contradictory ways, and companies must comply with each.

In many cases, the directive does not take into account the global nature of data and the way in which data is collected, used, stored and shared. It requires that data only be transferred to countries found by the Commission to provide adequate protections for personal data. Fewer than 10 countries have been found to be adequate. While other legal mechanisms are available to support the transfer of data under the directive, as we heard earlier today, they are cumbersome.

Finally, the directive's requirement that organizations have a legal basis to process data can impose additional burdens without yielding good privacy outcomes. In the United States, companies can use data unless they are specifically prohibited from doing so. In Europe, by contrast, companies are not allowed to process data unless the processing meets one of six criteria found in the directive.

The most significant of these criteria is informed consent of the data subject. To obtain consent, companies must specify in the privacy policy the purpose for which data will be processed. However, the ways in which data can be used evolve rapidly and may not be readily foreseen by companies. When data holds such broad and unanticipated potential, companies will hesitate to specify its criteria for processing for fear of limiting their options in the future. Companies instead may create broad privacy policies aimed at obtaining permission to undertake any data activity they see fit.

What is at issue is not the value of privacy protection nor that of fair information practices. They continue to serve as the most respected and trusted foundation for privacy protection. What requires our consideration is how quickly the fair information practices are applied in this new and rapidly changing data environment and how companies and regulators faced with the need to make the best possible use of scarce resources can be empowered to direct time, funding and personnel towards efforts that yield optimal privacy for individuals without unduly constraining innovation.

In a digital age, in an economy driven by data, getting privacy protection rights is hard. There are no simple solutions. Policy makers, industry leaders, regulators and advocates are engaging in discussions here in the U.S. and in international forums to develop approaches that serve both organizations that collect data and the privacy of individuals. Therefore, as this committee continues to explore this issue, I encourage you to consider the alternatives

developed in these ongoing discussions.

Thank you again for this opportunity, and I look forward to answering any questions.

[The prepared statement of Ms. Bruening follows:]

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

Mrs. Bono Mack. Thank you very much, Ms. Bruening.

And Professor Swire, you are recognized for 5 minutes.

STATEMENT OF PETER P. SWIRE

Mr. Swire. Thank you, Madam Chairman and Ranking Member Butterfield, and other distinguished members of the committee. Thank you for inviting me to participate today.

This is an area that has long been of great interest to me. I wrote a book on the U.S. and EU privacy laws back in the nineties. I was chief counselor for privacy under President Clinton and helped to negotiate the Safe Harbor agreement that have we heard about today.

Before turning to my written testimony, just a brief comment on the very important research that Professor Tucker has talked about today. This is incredibly useful data, but I would like you to think about advertising being targeted. We could do it even better if we saw every e-mail you saw, every text message you ever wrote, every moment-by-moment location information. We could target better, but having all of that known to the advertisers creates some risks and I think we probably would want to have privacy and have good business not just maximize how much everybody sees about us.

In my written testimony there are three points. I will focus on the third one today. The first point is that the EU Data Protection Directive has deep roots in the United States history of privacy protection. The fair information practices came from here, and that

is what is built into the directive.

A second point is I have often criticized the EU directive in a number of details in my writing, but with that said, the European regime has made important contributions to our privacy practices. Many of the sensible ways that we self regulate today in the United States really grew out of discussions that were involved in European regulators, and we have taken the best of that in many cases to do good business and good privacy.

The focus of my time today, though, is going to be on jobs and U.S. businesses and the effects on those. My point here is that support for baseline privacy principles is good business and good policy for the United States. If we adopt a "we don't care about privacy" attitude, that creates major risks for American jobs, American exports, and American businesses. Other countries could then decide that the U.S. is a noncompliance zone, and they can ban transfers of data to the United States.

Foreign competitors can then use the lack of U.S. privacy protections as an excuse for protectionism and then insist that all the information processing happen in their countries and not here in the United States, where right now we have such an important technological edge.

So I am going to continue with a little more detail on some of those job and business effects.

The Safe Harbor, as was discussed earlier, is a big help for transferring data between EU and the United States, and we made the

European rules much more workable as we negotiated that. But the risk of protectionism is growing again. The EU is in the midst of a major revision of the directive. They may make it substantially stronger in some respects. And as the chairman noted, India's privacy laws are coming online now, Mexico and most of Latin America are adopting these laws, and right now they are copying the European approach. If we had a baseline approach in the United States that was simple and easy to communicate, I think it would be a lot easier for them to copy the U.S. approach or at least for us to have U.S. style principles accepted around the world. If we don't do that, we are risking having a very bad model become the practice generally.

RPTS JOHNSON

DCMN BURRELL

[12:20 p.m.]

Mr. Swire. [Continuing.] Cloud computing is just one industry that gives an example of the risks we face here. The Province of British Columbia few years ago canceled contracts because they thought sending data to the United States wasn't safe enough. There have been several discussions in European Parliaments this year that, similarly, having databases in the United States is not safe enough for the data of European citizens.

Now, when we have these important information services, cloud computing, Internet sales, other U.S. areas of leadership, we can't just ignore the rest of the world in this case. And here is why. Many of the U.S.-based companies have assets in these countries. We have employees in these countries. If Germany, which for instance one of the German States had a 60,000 euro fine this week about a financial firm for affiliate sharing. When the German regulators do this, they can go after American companies' assets overseas. We have seen that Italy has even gone against a Google employee on a criminal basis.

So we are stuck in a world where they have national jurisdiction and national legislation. I think the question then is how do we engage, how do we find a way for the United States to best have our self-regulatory, our good privacy principle, but our nonintrusive approaches, but also explain to the rest of the world how to stop this

protectionism.

I think we should maintain our own privacy legal structure. Baseline principles I think are the way to go, baseline legislation if possible. The risk is that we do so little that the rest of the world says we don't do enough at all and shuts us out. And I think that is something to avoid.

Thank you, Madam Chairman.

[The prepared statement of Mr. Swire follows:]

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

Mrs. Bono Mack. Thank you, Professor. I appreciate very much all of your testimony, and apologize for always having to rush to get it in under 5 minutes. But now I will recognize myself for the first 5 minutes of questioning.

Professor Tucker, to you, in your research how did you account for the difference between what European privacy regulations say on paper and then how they are actually enforced? And what does that difference mean for those who would suggest we model U.S. privacy regulations on European ones?

Ms. Tucker. So my study, because it is an empirical study, is really a study of how firms interpreted the laws, with all their ambiguity, all the lack of clarity, all the uncertainty. And when I talk to people about my results, what has been really emphasized to me is the extent when laws are written in a vague way and people don't really quite know what they mean, often counsel do urge the company to take a very conservative and cautious approach.

So I think one way, you know, of understanding that gap is if there is a gap between what was intended and what companies are doing, it often tends to be conservative, because companies obviously do not want the bad publicity associated of being found guilty of privacy violations.

Mrs. Bono Mack. Thank you. In your testimony you state you would like to see research that tests elements of a "do not track" technology, because your research shows some forms of consumer choice regarding their privacy can improve advertising effectiveness. Can

you explain further what you mean?

Ms. Tucker. Yes. So this is a separate study, where I actually looked at online advertising on Facebook. And you may remember a year ago Facebook was under a lot of pressure, and they actually implemented a whole new series of privacy controls. And what we saw is that when we actually gave users control over their own privacy and how their personal information was being used, that it has actually a large improvement in terms of how willing people were to click on relatively personalized advertising.

Mrs. Bono Mack. Thank you. And I kind of have a golden question. And I will go to you, Professor, and then let each of you take a swipe at this one. What questions do you all think need to be answered for us to understand how restrictions on data could affect digital media and services? And I will start with you, Professor Tucker, on that.

Ms. Tucker. Okay. So I feel -- I mean I am constantly frustrated by how little empirical research there is out there. And as a policymaker, we found it hugely difficult to try and say what matters and what doesn't in terms of actually affecting consumer response. So I think what we really need is more research on trying to understand, well, if we do have to have regulation, how can we make it good regulation which actually benefits firms and consumers at the same time? Thereby through giving trust, encouraging consumers to trust companies, and therefore getting some benefits, while hopefully not costing firms so greatly.

Mr. Pratt. You are right, that is a big question. So I think

the question I would ask, if I was sort of sitting up there rather than here, would be how all the innovation here that we see on the Internet really is U.S.-based. I think Professor Swire is right, we really have the edge as a country. It is because of the freedom that we have to have innovated that all these innovations are here that are moving around the world. But we also know that the Internet, all the free stuff, all the free stuff is monetized in some way. It is supported by an economy. And I think the key question, which I have heard in some other hearings, is so if we are going to strip away a lot of what supports, you know, what is the economy that supports the way that we interact with the Internet today, what takes its place and what is the consequence of a whole different system of billing individuals for participating in powerful tools, search engines, and so on and so forth? So I think this monetizing economy question is sort of fundamentally important.

But I would certainly agree that go slow and seek empirical answers is awfully important as well. So there is no reason to rush to some immediate conclusion.

Mrs. Bono Mack. Thank you. Ms. Bruening?

Ms. Bruening. Yes. I think it was acknowledged earlier today already that so much of what we think about privacy is very culturally based, it is based on history, and experience, and mores, and we are going to be hard pressed to convince one part of the world or another that our way is better. And we certainly don't want to adapt their approaches.

At the same time, global flows of data are critical to our economy, to the world economy. They have to be robust in order to keep economic growth going. And it is so necessary right now. So the question becomes how do we respect these divergent ideas about privacy and yet have an interoperable system that allows for those data flows? And I think trying to figure out how you create that system is going to be really, really important.

I think the other question is, you know, we keep hearing about how companies need more flexibility to process data than is perhaps allowed for in something like the directive. And even in many ways in the kinds of rules and regulations we have here in the United States. So again, how do you provide that flexibility in a way that also requires that companies assess the risks that they are raising for individuals when they are using that data, and that they mitigate those risks so that they are accountable for the way in which they are using data?

Mrs. Bono Mack. Thank you. Professor Swire, I apologize. My time has expired. But I know that some of my colleagues will jump to you. So I would like to recognize Mr. Butterfield for 5 minutes.

Mr. Butterfield. Thank you. Dr. Tucker, I thank you for your testimony. Obviously, it is very thoughtful. And I certainly don't want to make light of your research. And it is important research that can and should contribute to our decision-making process. But because those who oppose privacy legislation have touted it as their rationale for opposition, I want to summarize what we know.

This study looks at a universe of ads that are not very effective

to begin with. Then it concludes that those not very effective ads have become even less effective as a result of European countries' efforts to protect consumers' privacy. And so we need to certainly continue that conversation.

A couple years ago, Mr. Swire, the RAND Corporation authored a report reviewing the strengths and weaknesses of the EU's Data Protection Directive. The directive contains a set of data protection principles. Each of the 27 countries then has its own set of laws implementing those principles. One of the goals of the directive was to set out a framework to bring the laws of each individual country closer together so the EU could truly function as one market.

We are talking about 27 different sovereign countries. So at the end of the day, there were bound to have been some differences, around the edges at the very least, in how they interpret and carry out the directive. But the RAND report concludes that one of the strengths of the directive is that it has harmonized data protection principles, and to a certain extent enabled an internal market for personal data. It cites as evidence the implementation of legal rules across Europe that have greater compatibility than prior to the directive's introduction. In other words, the legal rules of each of those countries have come closer together than they were prior to the directive.

Professor, can you please comment, if you will, on this observation generally? And in particular, can you please discuss whether and how this convergence in the legal rules of 27 countries

has actually benefited the U.S. and other companies trying to do business in the European Union?

That is a very comprehensive question. You have a couple minutes to respond.

Mr. Swire. I won't take all your time. Thank you, Congressman.

When the directive was first being considered in the early 1990s, there were two big goals. One of the goals was to protect privacy, but the real driver was the Common Market, which is what you were talking about, which is there is supposed to be free flow of information between Italy and France and Germany, and now all the other countries. And so the directive was set up so that the ceiling and floor were supposed to be pretty close together. So it wasn't total preemption, it wasn't exactly the same everywhere, but if it had been a great big difference, now it is supposed to be a much, much smaller difference.

And we know in the United States we face this, your committee faces this on preemption for data breach and the rest. If the things are pretty darn close, a lot of time companies can deal with it. That is what the directive was supposed to do. In practice, it probably hasn't always achieved that. But that free flow of information within Europe was one of the two main goals for creating the whole thing.

Mr. Butterfield. Thank you. We still have some time. Professor, in your testimony you state that prior to implementation of the Safe Harbor agreement that you helped negotiate, there was widespread perception that American-based companies were subject to stricter privacy enforcement in Europe than EU-based companies. As

U.S. leaders, we, of course, hear about the problems faced by our companies in dealing with the regulatory regimes of other countries. And we, of course, hear complaints about unfair treatment and enforcement. And when it is a giant like Microsoft, Google, or Facebook, everyone is going to read and hear about it if an EU country goes after that.

Given all of this, sir, some of us might still be under the impression that the U.S. companies are treated differently and more strictly when it comes to enforcement of EU data protection rules. I think you know where I am going with that. Please help me with it.

Mr. Swire. I will try to help, sir.

Mr. Butterfield. Yes.

Mr. Swire. So my view is in the early period there was a highly visible focus on U.S.-based companies for enforcement. The enforcement action this week that I mentioned in Germany in the financial area was against a German company, dealing with German providers. And over time a far bigger fraction of enforcement actions, as I understand it, have been for European companies, and not focused on the U.S. We should always look for problems with that discriminatory treatment, and we should step in when we see it. But the point about discriminatory treatment is if we just say we don't care about privacy, it strengthens the hand of European enforcers who want to go after U.S. companies, because they think they can't trust it when the data comes here. So just saying we don't care or we don't do that here really raises the risk of focus on the U.S.

enforcement -- enforcement against U.S. companies.

Mr. Butterfield. So there is some perception of singling out of U.S. companies?

Mr. Swire. My sense is that you know, the home field advantage is quite important. I am from Ohio State, and we believe in the home field advantage. And you know, this sort of thing happens. And the U.S. Constitution has a diversity jurisdiction so that if you are out of State you get Federal judges to help you.

So that is a concern. But if we are able to keep showing that in the U.S. we do basically a solid job on privacy, then that is an enormous answer back to the people who want to be protectionist.

Mr. Butterfield. Thank you. Very helpful. Thank you.

Mrs. Bono Mack. I thank the gentleman. And the Professor would note that the chair is a U.S.C. Trojan grad.

Mr. Swire. Also a fine team, ma'am.

Mrs. Bono Mack. Thank you. The chair will recognize Mr. Stearns for 5 minutes.

Mr. Stearns. Thank you, Madam Chair. Dr. Tucker, it just seems to me it comes down to that there is two questions here. If we don't adopt privacy regulation like the European Union, then in a sense we are shut out of their market. And if other countries in Latin America and others that are taking the European Union as a standard and moving in that direction, then we have around us, whether it is Latin America, Europe, we have all these countries that are subscribing to the European Union model, then in a way we are disadvantaged.

So that is one question. And the other question is, though, that, you know, when you look at it, you know, Google, and Twitter, and YouTube, and Facebook, and Groupon, all these came because of the innovation here in the United States. It didn't come from Europe, it didn't come from Latin America. So if we adopt the European Union model that everything has to be opt-in, then the innovation that comes from behavioral advertising -- we all agree that financial and health records should be protected; that is okay -- but some of the behavioral advertising works to the benefit of the consumer. Groupon is a good example. You can get ads now that it will give you a discount on things that you might not have thought of, but it is in your behavioral interests. And so, you know, it is caught between those two, whether the United States succumbs to the European model and loses its innovation, or at the same time does the European Union -- we just say we are not going to do it, and continue our innovation, and who knows what will come up besides another Facebook or Twitter?

So I guess my question is do you believe there is a demonstrated harm to consumers from being tracked online for the purpose of being served targeted ads?

Ms. Tucker. Okay.

Mr. Stearns. Amen.

Ms. Tucker. Amen. Okay. So there is three questions embedded there.

Mr. Stearns. This is the only question I have.

Ms. Tucker. This is the only question.

Mr. Stearns. Because if you can show from your models or your empirical evidence that we are better off with innovation, then why don't we convince the Europeans to be like us? Which we can't do, but I understand.

Ms. Tucker. So we have tried to run some initial studies to see how customers respond to personalized advertising. We haven't seen any behavioral evidence they are navigating away, appear to be unhappy of being shown it. Beyond that --

Mr. Stearns. But can't you say there is substantial benefits to consumers from having this model that we have in the United States? Wouldn't you say that is true?

Ms. Tucker. Well, I mean in terms of how many wonderful free and innovative services are supported through advertising, I mean I would say definitely.

Mr. Stearns. Let me just go down. Mr. Pratt, do you have a comment on this question? Basically, is there a demonstrated harm to consumers from being tracked online for the purpose of being served targeted ads, in your opinion?

Mr. Pratt. You know, our world, the CDIA world, is the risk management world. But you know, you have no risk management decisions if you don't reach the right consumer with the right offer at the right time. So it begins with how we reach consumers. And in all parts of our industry, even in the CDIA's member, consumers are online more than ever before. When consumers get free credit reports, they go online to get them. So the bottom line is it is desperately important that

we have very effective mechanisms for connecting consumers with products. It empowers businesses. It is a home run, in my opinion. So you have got to have it. We do have it. We should be really careful about how we do harm to it.

Mr. Stearns. And you would not favor the European model?

Mr. Pratt. Well, we don't. You have heard that in our testimony. We are unequivocally opposed to importing that.

Mr. Stearns. All right. Ms. Bruening?

Ms. Bruening. I have not seen any empirical evidence about harm to consumers based on behavioral targeting. What I would say, though, is that the way we define harm in the United States is fairly circumscribed. We talk about it in terms of physical harm, financial harm. I think there is a growing recognition that harm may take different forms, that reputational harm, I think with the advent of social networking, has shown us that there are other harms involved. Reputational harm is one of them. I think there is a concern amongst consumers about how much data is being collected about them and how it is being used, and that there is not enough clarity about that.

So to say, you know, that there has been empirical evidence, I have not seen that, but I would not say that there is no harm at all if that is -- if that is a practice that there is not the appropriate assessment of risk and mitigation of risk on the part of companies who are engaging in it.

Mr. Stearns. Professor Swire?

Mr. Swire. Yes. Is there any harm to consumers? One answer is

it is a reason to have effective data breach protection.

Mr. Stearns. The question is more is there demonstrated harm to consumers that you have seen?

Mr. Swire. I think the demonstrated harm comes when there is data breaches and all the information about me gets leaked out. And then with the identity --

Mr. Stearns. But that is a security problem, not necessarily a privacy problem.

Mr. Swire. If everything is in the database, there is a bigger risk when it gets leaked.

Mr. Stearns. But if we have a good data security bill, and we say to the companies that you have to have a security officer, and you have to have it encrypted, and you have to be protected, that is different than just having behavioral advertising out there in which customers use it to buy things. So I am just asking have you found any demonstrated harm, any empirical --

Mr. Swire. I pointed to the biggest harm, which is when it leaks out.

Mr. Stearns. All right. Thank you, Madam Chair.

Mrs. Bono Mack. Thank the gentleman. And now recognize Mr. Pompeo for 5 minutes.

Mr. Pompeo. I will waive.

Mrs. Bono Mack. And he waives. And Ms. Blackburn for 5 minutes.

Mrs. Blackburn. Thank you, Madam Chairman. And I apologize to

you and the witnesses for being late to the hearing. I had a mandatory meeting that ran long, and I was a little bit detained. I do have a couple of articles that I want to submit for the record. They are from Financial Times. One is, Companies in Confusion Over Cookie Laws, and the other is Dutch Cookie Law May Lead to Online Exodus. And I would ask to submit those for the record.

Mrs. Bono Mack. Without objection.

[The information follows:]

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

Mrs. Blackburn. Thank you. I think that as Mr. Pratt said earlier, most of the innovation that has taken place in the digital revolution has come from here in the U.S. And I think there is no mistake in what that reason is. And that you can look at what is happening with the EU model, and it does cause you to back up and say, you know, if our job -- if our goal is to grow jobs, to expand the virtual marketplace, the virtual economy, then we are going to need to continue with a more flexible approach and make certain that we are protecting data, but that also we are allowing the use of that data in some ways.

I think the lack of implementation and variance in local interpretations on this cookie law, from what I have read, creates incredible uncertainty. And one of the things we are hearing right now from employers is they don't like the amount of regulatory uncertainty that is coming out of Washington because they don't know what their next step should be. And they also don't like the compliance cost, that there is an uncertainty built into that also.

So Mr. Pratt and Ms. Bruening, I would like for you to talk for just a little bit about the impact that the uncertainty and the rising compliance costs have on business. And then Dr. Tucker, as you address that, I want to go back to something that Mr. Butterfield was saying. And let's talk about the multinational companies and what you are seeing with what the application is to them. What is the cost to them? What is the lost opportunity cost that is going to be there to those multinational companies? And then for your companies that are local European companies, how are they going to lose out? So Ms. Bruening,

to you first, and then to Mr. Pratt, and then to Dr. Tucker.

Ms. Bruening. Thank you. I would say that the biggest indication of the concerns of businesses about uncertainty and compliance costs is the what we see at the Centre for Information Policy Leadership is their continued engagement in processes and deliberations internationally that would help to create more streamlined approaches to compliance. I think that many leadership companies are spending a great deal of time and resources engaging in processes at APEC. We are leading an international project on accountability that we have participants from the EU, North America, and Asia working on this with us, trying to figure out ways to make compliance more streamlined, to make it more certain, to give companies more flexibility, but also provide the appropriate privacy protections.

Mrs. Blackburn. Great. Mr. Pratt?

Mr. Pratt. I think the greatest uncertainty we could insert into the U.S. would be to create an umbrella entity, which is really what you have in Europe and in the various European Union member countries, and that is a data protection authority that essentially by fiat can make any decision about any data flow. To me, this is just abrogating the Congressional responsibility to legislate. It is empowering a regulator to then make decisions about commerce in a way that I just think is unhealthy. That kind of uncertainty makes it hard to innovate. You don't innovate first. You go to your lawyers and say what do you think they are going to say? And then maybe you build that

product, maybe you don't. Maybe you roll the dice, maybe you don't. And I think it begins to impinge on the freedom to innovate.

That is one of the many reasons why we don't think the European model is a good one to look at. We are not isolationists. We deal with the international dialogues. We have members who support these very international dialogues that she is referring to. We participated, actually, as a private company, as a private trade association in the EU Safe Harbor negotiations that took place way back when. We want data flows. We want that competition for our U.S.-based companies as well. We are global companies. But let's just make sure that we don't stifle what has been best.

Mrs. Blackburn. Dr. Tucker?

Ms. Tucker. So quickly, as we are out of time, the firms that have been really hurt have been the small firms on two dimensions. First of all, it is expensive to try and work out what these laws mean. Secondly, if you are a small start-up Web site, you are trying to get customers to opt in. When they are uncertain about whether or not to opt in, it is going to be harder for you to get that kind of consent.

Mrs. Blackburn. Thank you. Yield back.

Mrs. Bono Mack. I thank the gentlelady, and am happy to note it looks like we have concluded the hearing before the floor votes. I would like to thank the panelists all very much. It is clear that everybody in this room has learned something today, and cares deeply about these issues as we move these forward.

This was our second in a series of privacy hearings that we will

be holding this year. I look forward to our continued discussions on how we can best balance the need to remain innovative with the need to protect consumer privacy.

I remind members that they have 10 business days to submit further questions for the record. And I ask the witnesses to please respond promptly to any questions they receive.

Mr. Butterfield. Madam Chairman?

Mrs. Bono Mack. Yes.

Mr. Butterfield. May I be recognized for the purpose of offering a letter into the record, please?

Mrs. Bono Mack. The gentleman is recognized.

Mr. Butterfield. I have a letter in my possession from the TransAtlantic Consumer Dialogue addressed to the chairman and to the ranking member. I ask unanimous consent that it be included in the record.

Mrs. Bono Mack. Without objection.

[The information follows:]

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

Mrs. Bono Mack. And again, the hearing is now adjourned. Thank you all very much.

[Whereupon, at 12:42 p.m., the subcommittee was adjourned.]