AUTHENTICATED
U.S. GOVERNMENT
INFORMATION
GPO

INTERNET PRIVACY: THE IMPACT AND BURDEN OF EU REGULATION

HEARING

BEFORE THE

SUBCOMMITTEE ON COMMERCE, MANUFACTURING, AND TRADE

OF THE

COMMITTEE ON ENERGY AND COMMERCE
HOUSE OF REPRESENTATIVES

ONE HUNDRED TWELFTH CONGRESS

FIRST SESSION

SEPTEMBER 15, 2011

Serial No. 112–86

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

U.S. GOVERNMENT PRINTING OFFICE
73–961 PDF WASHINGTON : 2012

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

COMMITTEE ON ENERGY AND COMMERCE

FRED UPTON, Michigan
Chairman

JOE BARTON, Texas
Chairman Emeritus
CLIFF STEARNS, Florida
ED WHITFIELD, Kentucky
JOHN SHIMKUS, Illinois
JOSEPH R. PITTS, Pennsylvania
MARY BONO MACK, California
GREG WALDEN, Oregon
LEE TERRY, Nebraska
MIKE ROGERS, Michigan
SUE WILKINS MYRICK, North Carolina
Vice Chairman
JOHN SULLIVAN, Oklahoma
TIM MURPHY, Pennsylvania
MICHAEL C. BURGESS, Texas
MARSHA BLACKBURN, Tennessee
BRIAN P. BILBRAY, California
CHARLES F. BASS, New Hampshire
PHIL GINGREY, Georgia
STEVE SCALISE, Louisiana
ROBERT E. LATTA, Ohio
CATHY MCMORRIS RODGERS, Washington
GREGG HARPER, Mississippi
LEONARD LANCE, New Jersey
BILL CASSIDY, Louisiana
BRETT GUTHRIE, Kentucky
PETE OLSON, Texas
DAVID B. MCKINLEY, West Virginia
CORY GARDNER, Colorado
MIKE POMPEO, Kansas
ADAM KINZINGER, Illinois
H. MORGAN GRIFFITH, Virginia

HENRY A. WAXMAN, California
Ranking Member
JOHN D. DINGELL, Michigan
Chairman Emeritus
EDWARD J. MARKEY, Massachusetts
EDOLPHUS TOWNS, New York
FRANK PALLONE, JR., New Jersey
BOBBY L. RUSH, Illinois
ANNA G. ESHOO, California
ELIOT L. ENGEL, New York
GENE GREEN, Texas
DIANA DEGETTE, Colorado
LOIS CAPPS, California
MICHAEL F. DOYLE, Pennsylvania
JANICE D. SCHAKOWSKY, Illinois
CHARLES A. GONZALEZ, Texas
JAY INSLEE, Washington
TAMMY BALDWIN, Wisconsin
MIKE ROSS, Arkansas
JIM MATHESON, Utah
G.K. BUTTERFIELD, North Carolina
JOHN BARROW, Georgia
DORIS O. MATSUI, California
DONNA M. CHRISTENSEN, Virgin Islands
KATHY CASTOR, Florida

SUBCOMMITTEE ON COMMERCE, MANUFACTURING, AND TRADE

MARY BONO MACK, California
Chairman

MARSHA BLACKBURN, Tennessee
Vice Chairman
CLIFF STEARNS, Florida
CHARLES F. BASS, New Hampshire
GREGG HARPER, Mississippi
LEONARD LANCE, New Jersey
BILL CASSIDY, Louisiana
BRETT GUTHRIE, Kentucky
PETE OLSON, Texas
DAVID B. MCKINLEY, West Virginia
MIKE POMPEO, Kansas
ADAM KINZINGER, Illinois
JOE BARTON, Texas
FRED UPTON, Michigan *(ex officio)*

G.K. BUTTERFIELD, North Carolina
Ranking Member
CHARLES A. GONZALEZ, Texas
JIM MATHESON, Utah
JOHN D. DINGELL, Michigan
EDOLPHUS TOWNS, New York
BOBBY L. RUSH, Illinois
JANICE D. SCHAKOWSKY, Illinois
MIKE ROSS, Arkansas
HENRY A. WAXMAN, California *(ex officio)*

C O N T E N T S

	Page
Hon. Mary Bono Mack, a Representative in Congress from the State of California, opening statement	1
Prepared statement	4
Hon. G.K. Butterfield, a Representative in Congress from the State of North Carolina, opening statement	6
Hon. Pete Olson, a Representative in Congress from the State of Texas, opening statement	7

WITNESSES

Nicole Y. Lamb-Hale, Assistant Secretary for Manufacturing and Services, International Trade Administration, Department of Commerce	7
Prepared statement	10
Catherine Tucker, Douglas Drane Career Development Professor in IT and Management and Associate Professor of Marketing, MIT Sloan School of Management	22
Prepared statement	24
Stuart K. Pratt, President, Consumer Data Industry Association	34
Prepared statement	36
Paula J. Bruening, Vice President, Global Policy, Center for Information Policy Leadership, Hunton & Williams, LLP	52
Prepared statement	54
Peter P. Swire, C. William O'Neill Professor in Law and Judicial Administration, Moritz College of Law, The Ohio State University	65
Prepared statement	67

SUBMITTED MATERIAL

Article, "Companies in confusion over 'cookie' laws," by Maija Palmer for Financial Times, May 25, 2011, submitted by Mrs. Blackburn	81
Article, "Dutch cookie law may lead to online exodus," by Matt Steinglass for Financial Times, June 21, 2011, submitted by Mrs. Blackburn	83
Letter, dated September 14, 2011, from Julian Knott, Head of Secretariat, Trans Atlantic Consumer Dialogue, to subcommittee leadership, submitted by Mr. Butterfield	87

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, DC.

The subcommittee met, pursuant to call, at 11:18 a.m., in room 2322, Rayburn House Office Building, Hon. Mary Bono Mack (chairman of the subcommittee) presiding.

Members present: Representatives Bono Mack, Blackburn, Stearns, Bass, 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.

OPENING STATEMENT OF HON. MARY BONO MACK, A REPRESENTATIVE IN CONGRESS FROM THE STATE OF CALIFORNIA

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 became 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 rang-

ing 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.

[The prepared statement of Mrs. Bono Mack follows:]

Opening Statement of the Honorable Mary Bono Mack
Subcommittee on Commerce, Manufacturing, and Trade
"Internet Privacy: The Impact and Burden of EU Regulation"
September 15, 2011
(As Prepared for Delivery)

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 this 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's doing enough to protect American consumers, while government, unfortunately, tends to overreach every time it gets involved in the marketplace. From my perspective, there's 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's still a Wild, Wild West feel to cyberspace, leaving many consumers wondering if there's a Sheriff in town or whether they're 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 affect 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 privacy 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's the sweet spot we should be searching for in our hearings. Additionally, I will continue to work with Members of 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 European Union'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 on data privacy protections within the European Union, 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 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's 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. 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 protect privacy online and promote e-commerce. In the end, this will benefit both American consumers and American businesses, and preserve a strongly-held belief all across America that the Internet should remain free.

###

Mrs. BONO MACK. 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.

OPENING STATEMENT OF HON. G.K. BUTTERFIELD, A REPRESENTATIVE IN CONGRESS FROM THE STATE OF NORTH CAROLINA

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 privacy 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 1½ minutes to the gentleman from Texas, Mr. Olson, for his opening statement.

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

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.

We 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 NICOLE Y. LAMB–HALE, ASSISTANT SECRETARY FOR MANUFACTURING AND SERVICES, INTERNATIONAL TRADE ADMINISTRATION, DEPARTMENT OF COMMERCE

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:]

Testimony of
Nicole Y. Lamb-Hale, Assistant Secretary for Manufacturing and Services,
International Trade Administration, U.S. Department of Commerce
Before the House Energy and Commerce Subcommittee on Commerce,
Manufacturing and Trade
Internet Privacy: The Impact and Burden of EU Regulation
September 15, 2011

I. Introduction.

Good Morning, Madame 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 (EU) legal framework for data protection has on U.S. companies doing business in one or more of the EU member states. My testimony is particularly timely in light of the fact that the Department's Internet Policy Task Force has received feedback from industry and consumers that an enhanced U.S. privacy framework would facilitate mutual recognition of commercial data privacy laws around the world, thereby increasing practical protection for consumers and the reduction of barriers and compliance costs for U.S. companies in international markets.[1] In my capacity as the 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 United States, in particular, the U.S. Department of Commerce (Department) is doing to facilitate unencumbered transatlantic trade.

II. The European Union and United States' legal regimes for data protection and privacy

The EU and the United States share common goals in desiring to protect individuals' privacy while pursuing economic growth through increased trade and investment and by supporting Internet innovation. We arrived at these shared goals through over thirty years of transatlantic dialogue, beginning in the 1970s with the enactment of early data privacy laws in the US, Europe, and other democracies around the world. Our understanding and implementation of these common principles is influenced, however, by different historical perspectives and underlying differences in regulatory philosophy of our legal systems. Both these similarities and differences have influenced the developments of our respective data privacy legal frameworks.

EU Directive 95/46/EC on the protection of individuals with regard to the processing of personal data and on the free movement of such data, otherwise known as the EU Data Protection Directive, was issued by the European Parliament and the EU Council in 1995, and is currently under review. The Directive is drawn in part from the 1980 Organization for Economic

[1] All comments received by the Department in response to its Notice of Inquiry on the impact of privacy laws on innovation are available at http://www.ntia.doc.gov/federal-register-notices/2010/information-privacy-and-innovation-internet-economy-notice.

Cooperation and Development Guidelines (OECD Guidelines) on the Protection of Privacy and Transborder Data flows of Personal Data, which was endorsed by the United States and other OECD member countries, and provides a shared foundational understanding of key commercial data privacy rights and obligations among OECD countries. In the EU, the protection of personal data is included in the Charter of Fundamental Rights and the EU Data Protection Directive (EU Directive) provides the legal basis for protection of European citizens' personal data and privacy upon which national laws of the EU member states have been enacted. The EU Directive functions as a baseline for EU member states and allows them to adopt more stringent national protections. Additionally, Directive 2002/58 on Privacy and Electronic Communications, otherwise known as the E-Privacy Directive, complements the EU Directive, focusing specifically on protecting the privacy of Europeans active in the online environment. The EU amended this directive in 2009 to add requirements related to security breaches, spyware, cookies, and spam.

In the United States, the protection of individual privacy is deeply embedded in law and policy. The current legal framework consists of constitutional rights, common law, consumer protection statutes, and sector-specific laws such as the Health Insurance Portability and Accountability Act (HIPAA), the Gramm-Leach-Bliley Act (GLBA), and the Electronic Communications Privacy Act (ECPA). The various laws are enforced by the states, the courts, and by federal agencies such as the Federal Trade Commission (FTC). Voluntary multi-stakeholder policy development complements this framework.

This framework has encouraged innovation and provided many effective privacy protections. Focused civil and criminal law enforcement is applied when intervention is necessary to mitigate harm to the consumer. In particular, the FTC has been enforcing certain online consumer privacy protection through Section 5 of the FTC Act, which prohibits unfair or deceptive acts or practices. The states have additional consumer protection statutes. Supplementing this legal framework and government enforcement is a mix of self-regulating oversight organizations, trustmark seal programs, and codes of conduct. 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, and as Assistant Secretary Strickling noted in his testimony before this Committee on July 14th, the Administration is advocating for stronger consumer protection in the on-line environment.

III. How U.S. Companies Navigate EU's Privacy Framework

In the international context, the EU Directive imposes limitations on cross border data flows to countries whose legal frameworks do not meet its adequacy requirements as determined by the European Commission (EC), the executive arm of the EU. In 1998, the Department embarked on a two-year negotiating process with the 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 (Safe Harbor Framework), a policy approach that the EC deemed adequate in a July 26, 2000 finding. The Framework remains in force today.

The U.S.-EU Safe Harbor Framework went into effect on November 1, 2000. It is administered by the Department's International Trade Administration (ITA) on behalf of the United States. The Safe Harbor Framework is comprised of seven privacy principles, modeled on the OECD Guidelines and the EU Directive, as well as 15 FAQs that provide explanatory guidance to interested parties. The Safe Harbor Framework is a voluntary arrangement under which U.S. commercial entities may seek to undertake to comply with the framework principles and publicly declare they will do so. The Department maintains a website that provides a wealth of information to the business community on the elements of the program, the application process, renewal, and links to the EU's data protection unit under the Directorate General for Justice (DG Justice), the oversight authority in the EC. It also maintains a list of those U.S. firms that have self-certified their adherence to the Safe Harbor principles.

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 we add more than 60 new members each month. This service has enabled small and medium-sized 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 directly with the EU's legal framework. Onward data transfers are covered by the Safe Harbor Framework's onward transfer principle and allow organizations to move data to secondary processors. An estimated half trillion dollars in transatlantic trade is facilitated by the Safe Harbor Framework.

We have received assurances from the EC that the Safe Harbor Framework will continue to be a viable option for U.S. companies even as the EU revises its Directive. The Safe Harbor Framework is important to U.S. companies and their EU partners who rely on U.S. information technology service providers to provide state-of-the art products to their customers. The advent of cloud computing services in the EU presents its own set of challenges and we work regularly with our counterparts in the EC and at the member state level to clarify how personal data is protected in the "cloud."

Some large U.S. multinational corporations have chosen to avail themselves of alternative means of complying with the Directive, but these have proven to be costly and time-consuming. For example, several large U.S.-based multinational corporations have chosen to use binding corporate rules (BCRs), which permit global intra-corporate data flows 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 costs and time associated with obtaining approval of the BCRs are substantial. That may be why only very large multinational corporations use BCRs to comply with EU data protection laws.

Generally speaking, the biggest problems U.S. companies face with regard to navigating the privacy landscape in Europe include: 1) the significant resources that must be allocated to comply with these regulations (if they are not in Safe Harbor); 2) 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, 3) the differing EU member state regulations create legal uncertainty which complicates U.S. companies' efforts to plan for

the future. In addition, several U.S. companies – including cloud computing and social networking companies – have faced numerous challenges in the EU with regard to their business models and their privacy practices. Some of these challenges are a result of confusing requirements in the various member states.

IV. How the Department of Commerce Is Working Toward Greater Interoperability with the EU Privacy Framework

During testimony given at March and June hearings of the United States Senate Committee on Commerce, Science, and Transportation, my colleagues from the Department announced the Administration's support for legislation that would create baseline consumer data privacy protections through a "consumer privacy bill of rights." The Administration has been developing its views in more detail in a "White Paper" on consumer data privacy, which we hope to finalize this fall. One of the important concepts included in this paper is the need for greater interoperability of global commercial data privacy regimes.

While the Safe Harbor Framework has proven 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. Some companies in these sectors have indicated that they would like to see an improved environment for transatlantic data transfers.

The Department continues to engage the EU and its member states in discussions on how we can facilitate commercial data flows while at the same time respecting each other's laws and values. As Assistant Secretary Strickling noted in his testimony before this Committee on July 14, the Department has engaged in extensive conversations with EU data protection officials at all levels during the more than 10 years since the EU Directive entered into force. We have frequently engaged with senior officials from the EC, the European Data Protection Supervisor, members of the European Parliament, and national data protection commissioners. These interactions have been designed to convey to the EU that the U.S. legal framework, albeit structured differently, is as robust as the EU's framework for protecting individuals' privacy.

To build on the success of the Safe Harbor Framework, we hope to develop additional mechanisms that support mutual recognition of legal regimes, facilitate the free flow of information, and address emerging challenges. Specifically, we are considering the establishment of a multi-stakeholder process to produce enforceable codes of conduct that companies would then choose to adopt. In an open forum convened by the government, stakeholders with an interest in a specific market or business context will work toward consensus on a legally enforceable code of conduct that implements the Consumer Privacy Bill of Rights and other protections as appropriate. Under our proposed privacy framework, codes of conduct developed through this process would be enforced by the FTC, a world-leading privacy and consumer protection enforcement authority.

We in the Department believe that well-crafted multi-stakeholder consultation processes for Internet policy making are essential because they can nimbly respond to new challenges,

which in turn fosters confidence and clarity for consumers, industry, and other stakeholders. The attributes of speed, flexibility and decentralized problem-solving promoted by such multi-stakeholder consultations offer many advantages over traditional government rulemaking when it comes to establishing rules and guidelines that promote innovation and effectively protect consumers.

It is for this reason that the Administration supports a three-part legislative framework for consumer data privacy that includes principles-based privacy protections in the commercial sectors that are not subject to existing Federal data privacy statutes, encouragement for codes of conduct developed through a multi-stakeholder approach, and enhanced consumer data privacy enforcement authority for the FTC. The challenge is to find a way forward that allows this dynamic and stakeholder-driven process to reduce barriers to cross border data flow, but that is based on enhanced protections. We hope to include European stakeholders in our multi-stakeholder processes. While differences between the U.S. and EU commercial data privacy framework exist, our goals remain congruent. We both seek to protect individual consumers' personal information while promoting the appropriate free flow of information and global trade.

V. Conclusion

Thank you for the opportunity to explain how the EU's privacy and data protection framework relates to the commercial interests of the United States, to explain what the Department of Commerce is doing to help U.S. companies navigate privacy regulations in the EU, and to promote a legislative framework for consumer data privacy that continues to protect their privacy without stifling innovation and trade.

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 U.S. 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 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 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.

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.

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 atS 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 CATHERINE TUCKER, DOUGLAS DRANE CAREER DEVELOPMENT PROFESSOR IN IT AND MANAGEMENT AND ASSOCIATE PROFESSOR OF MARKETING, MIT SLOAN SCHOOL OF MANAGEMENT; STUART K. PRATT, PRESIDENT, CONSUMER DATA INDUSTRY ASSOCIATION; PAULA J. BRUENING, VICE PRESIDENT, GLOBAL POLICY, 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 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:]

MIT SLOAN

TESTIMONY

COMMITTEE ON ENERGY AND COMMERCE:
SUBCOMMITTEE ON COMMERCE, MANUFACTURING AND TRADE, U.S. HOUSE OF REPRESENTATIVES

Internet Privacy: The Impact and Burden of EU Regulation

CATHERINE TUCKER

September 15, 2011

Executive Summary

Currently the US is deliberating whether there is a need for privacy regulations governing internet commerce, and if there is a need, what form it should take. This is a tricky issue: There are risks to consumers if companies have unfettered access to consumers' data, but there is also a risk that strict regulations could damage the ability of internet firms to support free services through advertising. Given this delicate balance, it makes sense to try to understand the effects that privacy regulation has had in other countries.

My testimony will describe research I have carried out about how attempts by the European Union (EU) to protect privacy online has affected the performance of online advertising. I discuss three major findings of my empirical research:

(i) The EU's e-Privacy Directive was associated with a 65% decrease in the effectiveness of online advertising for the advertisers I studied.

(ii) The negative impact was not equal across websites. Ads on websites devoted to commercial product categories (such as travel and baby websites) were not affected. Ads on websites that had less commercial content such as news websites were most affected as they needed external consumer data to target ads effectively.

(iii) The negative impact was not equal across ads. Ads that were flashy and obtrusive (such as ads that float over the webpage) were not affected. The ads that were affected were plain and unobtrusive small banner ads whose appeal depended on them being informative to their audience.

This is only one consequence of regulation, and there may have been other consequences to firms and consumers. However, on the basis of this evidence, it is reasonable to say that privacy regulation could have sizable effects for the advertising-supported internet. Crucially, the burden that regulation imposes on websites and advertisers will not be uniform. Instead, the burden will be borne most by websites that have content that is not obviously commercial and advertisers who use less visually arresting advertising.

Consumer internet data is at the core of internet advertising but this raises privacy concerns.

Chairman Bono Mack, Ranking Member Butterfield, and Members of the Subcommittee: I was honored to receive the invitation to appear before you today to discuss the topic of 'Internet Privacy: The Impact and Burden of EU Regulation'

My name is Catherine Tucker, and I am the Douglas Drane Career Development Professor in IT and Management and Associate Professor of Marketing at MIT Sloan. My remarks concern research that I have carried out into the effects of regulation designed to protect consumer privacy on the internet in Europe.

This research matters because the US is contemplating moving away from the current system of industry self-governance, toward a more regulation-based model.

There are evident risks to consumers if companies have unfettered access to their data and firms do not have to be transparent about how they use this data and with whom they share it. However, nobody wants strong regulations to lead to adverse or unintended effects either. The advertising-supported internet is a huge and still rapidly growing engine of innovation, and represents a significant part of most users' internet experience. However, a policy issue arises because at the heart of this industry is the detailed collection, parsing, and analysis of consumer data, often without consumers' consent or knowledge. This data allows firms to *target* their advertising to specific groups who might be most interested in their advertising. This data also allows firms to *measure* how well the advertising then performs as they track the subsequent behavior of users who were exposed to an ad (Goldfarb and Tucker, 2011a). Data on the online behavior of consumers has allowed companies to deliver online advertising in an extraordinarily precise fashion. For example, a Cadillac dealership can target advertising so that their ads are shown only to people who have been recently browsing high-end cars on car websites. Such behavioral targeting has obvious benefits

to advertisers because fewer ad impressions are wasted. Instead, advertisers focus their resources on the consumers most likely to be interested in the ads. For consumers, however, ads that are behaviorally targeted can appear unauthorized and even creepy.

Therefore, policymaking in the area of privacy regulation needs to be careful and fulfil the twin aims of protecting consumer privacy *and* ensuring that the advertising-supported internet continues to thrive.

Given these aims, it makes sense to look and consider the outcome of other countries' attempts at privacy regulation. I want to discuss a research paper that I wrote (jointly with Avi Goldfarb from the University of Toronto) that studies how the European e-Privacy Directive affected advertising performance. This study was published in January in 2011 in Management Science, which is a top journal in my field (Goldfarb and Tucker, 2011c).[1] A summary was also published in the Communications of the ACM (Goldfarb and Tucker, 2011b).

I use extensive data to study the effects of the European e-Privacy Directive.

I examined the effect of the EU 'Privacy and Electronic Communications Directive' (2002/58/EC–sometimes known as the 'e-Privacy Directive') on online advertising in Europe. Specifically, I looked at how user response to advertising changed in Europe after the Directive came into place relative to changes in user response to advertising in the US and elsewhere.

Several provisions of the Privacy Directive limited the ability of companies to track user behavior on the internet and therefore limited the ability of these companies to use this data to target advertising (Baumer et al., 2004). These changes put certain roadblocks in the way of the ability of the Cadillac dealership, in my earlier example, to collect and use data about consumers' browsing behavior on other websites.

[1]The FTC Staff Report on "Protecting Consumer Privacy in an Era of Rapid Change: A Proposed Framework for Businesses and Policymakers quotes my paper on page D-5 as providing some evidence about potentially negative consequences for advertising revenues of privacy regulation affecting online advertising.

The interpretation of this e-Privacy Directive has been somewhat controversial and unclear as it relates to behavioral targeting. For example, it is not clear whether the provision, which requires companies that use invisible online tracking devices to use them only with the 'knowledge' of consumers, means that companies need explicitly to obtain opt-in consent. This is one of the reasons why, in the recent 'Telecoms Reform Package,' the EU amended the current regulation to require a user's explicit consent before placing a cookie on a computer. Hence my analysis reflects both the actual provisions of the original Directive and business responses when there is ambiguity over how privacy regulation should be interpreted.

To measure online advertising effectiveness, I use a large amount of data from a marketing research company that ran various tests of online display ads across the world over 8 years. The research company developed a straightforward methodology named an 'a/b' test that permitted comparison of different advertising campaigns over time in order to allow advertisers to benchmark the effectiveness of different ads. In this 'a/b' test, some randomly selected people were exposed to the ad for a certain product, while others were simply exposed to a placebo ad, usually for a charity. The market research firm then surveyed both groups about their likelihood of purchasing the advertised product. This allows a clean measurement of the effect of the ad: Because these people are randomly selected, any increase in expressed purchase intent towards the product for the group exposed to the ad relative to those who were not exposed can be attributed to advertising. I use data on 3.3 million of these survey responses for 9,596 different online display advertising campaigns conducted on hundreds of different websites across many countries.

I find that privacy protection reduced advertising performance by 65%.

In Europe, after privacy protection was enacted, the difference in stated purchase intent between those who were exposed to ads and those who were not dropped by approximately 65 percent. There was no such change for ad effectiveness for countries outside the EU. In

other words, online advertising became much less effective in Europe relative to elsewhere after the regulation was enacted.

One possible explanation for this result is that my estimates reflect a change in attitudes among Europeans towards targeted advertising, rather than something that can be causally attributed to how the change in law affected websites. To examine this possibility, I looked at the behavior of Europeans on non-European websites and of non-Europeans on European websites. I found no drop in ad effectiveness for Europeans browsing non-European websites and a substantial drop in advertising effectiveness for non-Europeans browsing European websites. The drop I measured does not appear to be simply a result of changing consumer attitudes in Europe. Instead, it suggests that, coincident with the timing of the enactment of European privacy regulation, advertising at websites in Europe became less effective.

The negative effects of regulation were not uniform.

The 65 percent drop in effectiveness was driven by two types of ads:

(I) Ads that were placed on websites whose content did not relate obviously to any commercial product, for example, CNN.com and Dictionary.com

(II) Ads that were small and did not rely on striking ad design to gain attention

The following ads were not adversely affected by regulation

(I) Ads that were placed on websites that had content that was easily relatable to demand for a group of products, such as tripadvisor.com or babycenter.com

(II) Ads that were large or that had rich-media features that were designed to gain attention

This makes it likely that the adverse effect of any regulation is not uniform. Instead, the adverse effect will be borne most by websites that are, in a sense, less commercialized

- that is, websites that have content that is not easy to match with a product category and advertisers that have so far shunned 'highly visual' advertising. In the long run, it seems likely that regulation could lead to incentives for websites to switch to content that is more easily matched to products (as they cannot use behavioral targeting techniques to match a consumer to a product) and for advertisers to use more highly visual and potentially distracting ads.

There are other approaches to privacy regulation

There are potential effects (both positive and negative) of regulation that I do not study.

(a) Whether there were additional negative effects for advertisers because they were less able to measure the efficacy of online campaigns using customer browsing data.

(b) How consumers benefited.

(c) How many consumers were aware of the nature of the regulation.

(d) The campaigns I study are representative of those launched by large firms who had the resources to place ads on individual websites. I do not know how privacy regulation affected smaller firms or advertising networks.

(e) I do not know whether the change in advertising effectiveness affected advertising revenues. Theoretically this would depend heavily on substitution patterns between online and offline media. If websites are forced to reduced prices to reflect the drop in effectiveness to prevent advertisers from switching to other advertising markets, then advertising-supported internet sites will bear the burden of regulation. If advertisers are unwilling to switch, they will simply have to pay more to achieve the same level of effectiveness as before.

This might suggest the US needs alternative approaches to privacy regulation.

In their recent set of proposals (FTC, 2010), the Federal Trade Commission made the following proposal:

> The most practical method of providing such universal choice would likely involve the placement of a persistent setting, similar to a cookie, on the consumer's browser signaling the consumer's choices about being tracked and receiving targeted ads. Commission staff supports this approach, sometimes referred to as 'Do Not Track.'

Obviously this persistent 'opt-out' is a different approach from the EU regulation that I study. However, my estimates do suggest that one could reasonably expect a large drop in advertising effectiveness for consumers who do choose to opt-out of targeting. Therefore, the likely effects of the proposed regulation depend on the number of consumers who ultimately choose to opt-out.

Crucially, the empirical findings of this paper suggest that any decline in advertising effectiveness that results from the new regulation will not be borne equally by all websites, and that the costs should be weighed against the benefits to consumers. In the long run, this may change the kind of websites and firms that prosper on the advertising-supported internet. My results also suggest that advertisers may move towards more visually arresting types of advertising in order to compensate for their inability to target.

The precise form of the new regulation will matter. Extensive efforts should be taken to collect data and encourage research that illuminates the burden that different forms of privacy regulation would impose on advertisers, consumers and websites. In particular, it would be attractive to test out elements of a 'do not track technology' that would encourage consumer choice regarding their privacy. This is because my own research indicates that some

forms of consumer choices regarding their privacy can actually improve the performance of advertising.

In another paper Tucker (2011), I present evidence that after Facebook introduced its new privacy settings that allowed more control over personally identifiable information click-through rates for personalized advertising actually increased. This suggests that if consumers are given choices over how advertising is geared to them, there can actually be an improvement in performance. However, I want to emphasize that this is only one study, and that far more research is needed to determine how the US can both protect consumers' privacy and the advertising-supported internet.

Thank-you for the opportunity to share these thoughts and I look forward to answering your questions.

References

Baumer, D. L., J. B. Earp, and J. C. Poindexter (2004). Internet privacy law: a comparison between the United States and the European Union. *Computers & Security 23*(5), 400 – 412.

FTC (2010, December). Protecting consumer privacy in an era of rapid change. *Staff Report*.

Goldfarb, A. and C. Tucker (2011a). *Advances in Computers*, Volume 81, Chapter Online Advertising. Elsevier.

Goldfarb, A. and C. Tucker (2011b, May). Online advertising, behavioral targeting, and privacy. *Communications of the ACM 54*, 25–27.

Goldfarb, A. and C. Tucker (2011c). Privacy regulation and online advertising. *Management Science 57*(1), 57–71.

Tucker, C. (2011). Social networks, personalized advertising, and privacy controls. *Mimeo, MIT*.

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:]

STATEMENT OF

STUART K. PRATT

CONSUMER DATA INDUSTRY ASSOCIATION

BEFORE THE

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

ON

"Internet Privacy: The Impact and Burdon of EU Regulation"

Thursday, September 15, 2011

1090 Vermont Avenue, NW, Washington, D.C. 20005
202-371-0910 Phone 202 371-0134 FAX

Chairman Bono-Mack, Ranking Member Butterfield, and members of the Subcommittee, my name is Stuart Pratt, and I am president and CEO of the Consumer Data Industry Association (CDIA). Thank you for this opportunity to testify.

CDIA is an international trade association with more than 190 member companies, providing our nation's businesses with the data tools necessary to manage risk in a wide range of consumer transactions. These products include credit and mortgage reports, identity verification tools, law enforcement investigative products, fraudulent check transaction identification systems, employment screening, tenant screening, depository account opening tools, decision sciences technologies, locator services and collections. Our members' data and the products and services based on it, ensure that consumers benefit from fair and safe transactions, broader competition and access to a market which is innovative and focused on their needs. We estimate that the industry's products are used in more than nine billion transactions per year.

My testimony today will focus on:

- Why it is important to preserve how consumer data is used in this country to protect consumers and enable US businesses to effectively manage risks.
- How US laws already protect consumers and successfully govern flows of data that are critical to the operation of our nation's economy.
- Why the fact that decisions about how to regulate the flow of data made by our country's trading partners and allies differ from those of the United States should

not stand as an argument for changing our country's approach to protecting consumers and enabling the most innovative data marketplace in the world.

CDIA MEMBERS' DATA AND TECHNOLOGIES HELP BOTH THE PUBLIC AND PRIVATE SECTORS TO PROTECT CONSUMERS AND MANAGE RISK

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 data bases, software and analytical tools are critical to how we manage risk in this country, ensure fair treatment and most importantly, how we protect consumers from becoming victims of both violent and white-collar crimes of all types.

In reviewing the following examples of how our members' products, software and databases protect consumers and mitigate risk you'll see why it is critical that we do not alter our domestic marketplace for consumer data and why our marketplace is such a success today. :

• Helping public and private sector investigators to prevent money laundering and terrorist financing.

• Ensuring lenders have best-in-class credit reports, credit scoring technologies, income verification tools and data on assets for purposes of making safe and sound underwriting decisions so that consumers are treated fairly and products make sense for them.

• Bringing transparency to the underlying value of collateralized debt obligations and in doing so ensuring our nation's money supply is adequate which militates against the possibility and severity of future economic crises.

• Enforcing child support orders through the use of sophisticated location tools so children of single parents have the resources they need.

• Assisting law enforcement and private agencies which locate missing and exploited children through location tools.

• Researching fugitives, assets held by individuals of interest through the use of investigative tools which allow law enforcement agencies tie together disparate data on given individuals and thus to most effectively target limited manpower resources.

• Witness location through use of location tools for all types of court proceedings.

• Reducing government expense through entitlement fraud prevention, eligibility determinations, and identity verification.

• Making available both local and nationwide background screening tools to ensure, for example, that pedophiles don't gain access to daycare centers or those convicted of driving while under the influence do not drive school buses or vans for elder care centers.

• Helping a local charity hospital to find individuals who have chosen to avoid paying bills when they have the ability to do so.

• Producing sophisticated background screening tools for security clearances, including those with national security implications.

• Improving disaster assistance responses through the use of cross-matched databases that help first-responders to quickly aid those in need and prevent fraudsters from gaming these efforts for personal gain.

Not only do our members' technologies and innovation protect us and ensure that we are managing risk in this country, but they reduce costs and labor intensity. Risk management is not merely the domain of the largest government agencies or corporations in America; it is available to companies of all sizes thanks to our members' investments. Consider the following scenarios:

Scenario 1 – Effective Use of Limited Resources

The following example was given during a Department of Homeland Security meeting on use of data by the department:

"One extremely well-known law enforcement intelligence example from immediately post 9/11 was when there was a now well-publicized threat…that there might be cells of terrorists training for scuba diving underwater bombing, similar to those that trained for 9/11 to fly – but not land – planes. How does the government best acquire that? The FBI applied the standard shoe- leather approach – spent millions of dollars sending out every agent in every office in the country to identify certified scuba training schools. The alternative could and should have been for the Federal government to be able to buy that data for a couple of hundred dollars from a commercial provider, and to use that baseline and law enforcement resources, starting with the commercial baseline."

Scenario 2 – Lowering Costs/Expanding Access to Best-in-Class Tools

One commercial database provider charges just $25 for an instant comprehensive search of multiple criminal record sources, including fugitive files, state and county criminal record repositories, proprietary criminal record information, and prison, parole and release files, representing more than 100 million criminal records across the United States. In contrast, an in-person, local search of one local courthouse for felony and misdemeanor records takes 3 business days and costs $16 plus courthouse fees. An in-person search of every county courthouse would cost $48,544 (3,034 county governments times $16). Similarly, a state sexual offender search costs just $9 and includes states that do not provide online registries of sexual offenders. An in-person search of sexual offender records in all 50 states would cost $800.

Scenario 3 – Preventing Identity Theft & Limiting Indebtedness

A national credit card issuer reports that they approve more than 19 million applications for credit every year. In fact they process more than 90,000 applications every day, with an approval rate of approximately sixty percent. This creditor reports that they identify one fraudulent account for every 1,613 applications approved. This means that the tools our members provided were preventing fraud in more than 99.9 percent of the transactions processed. These data also tell us that the lender is doing an effective job of approving consumers who truly qualify for credit and denying consumers who are overextended and should not increase their debt burdens.

CURRENT LAWS REGULATING DATA FLOWS PROTECT CONSUMERS AND ENCOURAGE INNOVATION

The United States is on the forefront of establishing sector-specific and enforceable laws regulating uses of personal information of many types. The list of laws is extensive and includes but is not limited to the Fair Credit Reporting Act (15 U.S.C. 1681 et seq.), The Gramm-Leach-Bliley Act (Pub. L. 106-102, Title V), the Health Insurance Portability and Accountability Act (Pub. L. 104-191), and the Drivers Privacy Protection Act (18 U.S.C. 2721 et seq.). CDIA believes this sector-by-sector approach has not just worked well, but has ensured that the United States has both marketplace that puts consumers first and one that is the most robust, innovative and effective. Following are more probative descriptions of some of these laws, the rights of consumers and also the types of products that fall within the scope of the law.

Fair Credit Reporting Act

Key to understanding the role of the FCRA is the fact that it regulates any use of personal information (whether obtained from a public or private source) defined as a consumer report. A consumer report is defined as data which is gathered and shared with a third party for a determination of a consumer's eligibility for enumerated permissible purposes.

This concept of an eligibility test is a key to understanding how FCRA regulates an extraordinarily broad range of personal information uses. The United States has a law which makes clear that any third-party-supplied data that is used to accept or deny, for example, my application for a government entitlement, employment, credit (e.g., student loans), insurance, and any other transaction initiated by the consumer where there is a legitimate business need. Again, this law applies equally to governmental uses and not

merely to the private sector and provides us as consumers with a full complement of rights to protect and empower us. Consider the following:

• The right of access – consumers may request at any time a disclosure of all information in their file at the time of the request. This right is enhanced by requirements that the cost of such disclosure must be free under a variety of circumstances including once per year upon request, where there is suspected fraud, where a consumer is unemployed and seeking employment, when a consumer places a fraud alert on his or her file, or where a consumer is receiving public assistance and thus would not have the means to pay. Note that the right of access is absolute since the term file is defined in the FCRA and it includes the base information from which a consumer report is produced.

• The right of correction – a consumer may dispute any information in the file. The right of dispute is absolute and no fee may be charged.

• The right to know who has seen or reviewed information in the consumer's file – as part of the right of access, a consumer must see all "inquiries" made to the file and these inquiries include the trade name of the consumer and upon request, a disclosure of contact information, if available, for any inquirer to the consumer's file.

• The right to deny use of the file except for transactions initiated by the consumer – consumers have the right to opt out of non- initiated transactions, such as a mailed offer for a new credit card.

• The right to be notified when a consumer report has been used to take an adverse action. This right ensures that I can act on all of the other rights enumerated above.

• Beyond the rights discussed above, with every disclosure of a file, consumers receive a notice providing a complete listing all consumer rights.

• Finally, all such products are regulated for accuracy with a "reasonable procedures to ensure maximum possible accuracy" standard. Further all sources which provide data to consumer reporting agencies must also adhere to a standard of accuracy which, as a result of the FACT Act, now includes new rulemaking powers for federal agencies.

Gramm-Leach-Bliley Act

Not all consumer data products are used for eligibility determinations regulated by the FCRA. Congress has applied different standards of protection that are appropriate to the use and the sensitivity of the data. We refer to these tools as Reference, Verification and Information services or RVI services. RVI services are used not only to identify fraud, but also to locate and verify information for the public and private sectors.

Fraud prevention systems, for example, aren't regulated under FCRA because no decision to approve or deny is made using these data. Annually businesses conduct an average more than 2.6 billion searches to check for fraudulent transactions. As the fraud problem has grown, industry has been forced to increase the complexity and

sophistication of the fraud detection tools they use. While fraud detection tools may differ, there are four key models used.

• Fraud databases – check for possible suspicious elements of customer information. These databases include past identities and records that have been used in known frauds, suspect phone numbers or addresses, and records of inconsistent issue dates of SSNs and the given birth years.

• Identity verification products – crosscheck for consistency in identifying information supplied by the consumer by utilizing other sources of known data about the consumer. Identity thieves must change pieces of information in their victim's files to avoid alerting others of their presence. Inconsistencies in name, address, or SSN associated with a name raise suspicions of possible fraud.

• Quantitative fraud prediction models – calculate fraud scores that predict the likelihood an application or proposed transaction is fraudulent. The power of these models is their ability to assess the cumulative significance of small inconsistencies or problems that may appear insignificant in isolation.

• Identity element approaches – use the analysis of pooled applications and other data to detect anomalies in typical business activity to identify potential fraudulent activity. These tools generally use anonymous consumer information to create macro-models of applications or credit card usage that deviates from normal information or spending

patterns, as well as a series of applications with a common work number or address but under different names, or even the identification and further attention to geographical areas where there are spikes in what may be fraudulent activity.

The largest users of fraud detection tools are financial businesses, accounting for approximately 78 percent of all users. However, there are many non- financial business uses for fraud detection tools. Users include:

• Governmental agencies – Fraud detection tools are used by the IRS to locate assets of tax evaders, state agencies to find individuals who owe child support, law enforcement to assist in investigations, and by various federal and state agencies for employment background checks.

• Private use – Journalists use fraud detection services to locate sources, attorneys to find witnesses, and individuals use them to do background checks on childcare providers. CDIA's members are also the leading location services providers in the United States. These products are also not regulated under FCRA since no decision is based on the data used. These services, which help users locate individuals, are a key business-to-business tool that creates great value for consumers and business alike. Locator services depend on a variety of matching elements. Consider the following examples of location service uses of a year's time:

• There were 5.5 million location searches conducted by child support enforcement agencies to enforce court orders. For example, the Financial Institution Data Match program required by the Personal Responsibility and Work Opportunity Reconciliation Act of 1996 (PL 104-193) led to the location of 700,000 delinquent individuals being linked to accounts worth nearly $2.5 billion.

• There were 378 million location searches used to enforce contractual obligations to pay debts.

• Tens of millions of searches were conducted by pension funds (location of beneficiaries), lawyers (witness location), blood donors organizations (blood supply safety), as well as by organizations focused on missing and exploited children.

Clearly our members are producing best-in-class data products and services that protect consumers, prevent crimes, mitigate risks and enable robust competition. US laws governing the flow of consumer data, such as the Gramm-Leach-Bliley Act and Fair Credit Reporting Act, are protective of consumer rights and also ensure that products used to protect consumers, prevent fraud and to locate individuals are allowed to operate for the good of consumers and business.

DATA FLOWS AND THE FUTURE

While some may think that the United States has been trying to catch up to the world when it comes to data flows and regulation, this is not the case. Well prior to the first OECD Fair Information Practices Guidelines of 1980 or any action taken by the European Union our country had enacted the Fair Credit Reporting Act which regulates

all third-party aggregated data used for making a decision about a consumer. Congress was prescient in this action. As discussed above our sector-by-sector approach to laws and regulations has not resulted in a dearth of protections for consumers or congressional oversight. Where laws have been needed congress has passed them. In fact there is an extraordinarily thorough record of congressional oversight of various industry sectors' uses of personal information. The U.S. has chosen a sector-specific structure to consumer data laws which ensures regulatory structures which are both appropriate to the data and which can be effectively enforced. Sector-specific laws and regulations exist today because of such oversight and due to the expertise of different committees overseeing different aspects of American business.

What is also clear is that there is not a homogeneous world view when it comes to how consumer data protection should be structured and 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 including just a few of the many listed below:

- The 1973 HEW Report contains 5 principles.
- The 1980 OECD Guidelines contain 8 principles.
- The 1995 EU Data Protection Directive contains 11 principles.
- The 2000 FTC Report on Online Privacy contains 4 principles; and
- The 2004 APEC Privacy Framework contains 9 principles.

Even in Europe the Data Protection Directive has been transposed into country-specific laws which, while perhaps determined as adequate by the EU, are still different. Today credit reporting is still a balkanized process that impinges on the theory of a single market for financial services competition. Consumers who move from one country to another may find that their credit reports are not portable and thus they start over and all of their historical hard work in managing their credit is lost. This example alone argues against the theory that there is a single theory or right answer when it comes to how consumer data should be protected.

New reports by the FTC and the Department of Commerce introduce ideas into the U.S. dialogue but they are not offered as final conclusions. International commentators question whether or not the current U.S. discussion will ineluctably lead to the theoretically important aspirational goal of harmonization with other privacy conventions such as that of Europe. Consider the following comment submitted to the U.S. Department of Commerce as indicative of this point:

> "From a European perspective, it is not clear whether these provisions apply to personal data in the public domain. The document supports the APEC Framework (recommendation 6), but that Framework does not apply to public domain personal data.
>
> This lack of clarity may create harmonisation difficulties re privacy matters and this position highlights one fundamental difference which helps explain why the USA's view of "privacy" is not the same as the European understanding of "data protection"."

CDIA's members operate on a global basis and are respectful of individual countries' traditions and values. Our members are the most successful companies in the world when it comes to producing data that protects consumers, allows for effective risk-management and which facilitate competition. Historical context, cultural mores, and much more drive an individual country's deliberations about how to protect its citizens' data and this is no less true here in the United States.

CDIA itself has participated in international task forces such as that recently hosted by the World Bank and International Bank of Settlements to work on international standards for credit reporting. This international dialogue recognized that standards operate above the particulars of various countries' legal regimes and necessarily so. It also recognized that trans-border data flows can be achieved outside of the ill-conceived theory of global harmonization of data protection.

The APEC discussions are yet again fundamentally demonstrative of the fact that the world actively seeks and finds ways to ensure international trade issues are addressed. Such regional trade discussions are respectful of national interests and law, while also exploring new answers to questions of how best to encourage our global economy to expand and benefit all involved.

CDIA offered its expertise to the Department of Commerce when it negotiated the Safe Harbor Agreement with Europe. Such dialogues demonstrate that there is no fundamental tension between preserving the importance of domestic laws that empower the U.S. economy and still finding a means of addressing the concerns of trading partner via mutually respectful discussions.

In closing, it is our view that our U.S. model has worked exceptionally well for our citizens and for our economy. We continue to support a sector-specific approach because:

- Laws resulting from this approach are far more likely to respect free speech rights in our constitution, an American value that cannot be subordinated to any external dialogue.
- Laws are more likely to be focused and overreaching in a manner that would impinge on innovation.
- Laws are subjected to the deliberations and oversight of congress which is obligated to represent the interests of the citizens of this country.
- Decisions about data protection are not an abrogation of congressional authority through the establishment of a new federal regulator with regulatory powers that overshadow on the legislative authority of the congress, itself.
- History has proven that our approach works well for our country and for our citizens.

Thank you for this opportunity to testify and I am happy to answer any questions.

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:]

Hearing on
Internet Privacy: The Impact and Burden of EU Regulation
September 15, 2011

Testimony of Paula J. Bruening
Vice President, Global Policy
Centre for Information Policy Leadership
Hunton & Williams LLP

before the
U.S. House of Representatives Committee on Energy and Commerce
Subcommittee on Commerce, Manufacturing and Technology

Distinguished Chairman, honorable committee members, I am Paula J. Bruening, Vice President for Global Policy of the Centre for Information Policy Leadership. I am honored to testify on The Internet: The Impact and Burden of the EU Regulation.

The Centre for Information Policy Leadership is a think tank and policy development organization located in the law firm of Hunton & Williams LLP. The Centre was established to develop innovative, pragmatic solutions to privacy and information security issues that reflect the dynamic and evolving nature of information-intensive business processes and at the same time respect the privacy interests of individuals. The Centre's member companies include leading organizations in health care, information services, retail, technology, financial services and consumer products.

Since its establishment, the Centre has addressed such issues as conflicting national legal requirements, cross-border data transfers and government use of private sector data, with a view to the impact of the future direction of business practices and emerging technologies on those issues. The Centre has spoken about these issues before the U.S. Department of Commerce, the Federal Trade Commission and congressional committees at workshops and hearings. It has been an active participant at the Organisation for Economic Co-operation and Development and

the Asia-Pacific Economic Cooperation forum. Currently the Centre leads the work of the Accountability Project, now concluding its third year. That project engages the expertise of an international group of government representatives, regulators, privacy experts, businesses and advocates to design a responsible, innovative approach to information privacy and data protection based on the fair information practice principle of accountability. The Centre's work has influenced privacy laws and regulation in the United States and abroad.

The Centre and its 41 member companies believe that difficult information policy issues must be resolved responsibly if we are to fully realize the benefits of an information economy. Centre experts and staff, however, speak only for themselves. As I prepared this testimony, I consulted with Centre colleagues and Centre members; however, my comments today reflect my views and do not necessarily reflect the views of Centre member companies, Hunton & Williams LLP, or any firm clients.

As we examine the question of the impact and burden of EU regulation, it is important to bear in mind that privacy laws are enacted in a manner consistent with local law and reflect the local culture of privacy. United States legal tradition differs markedly from that of Europe, and the American concept of privacy is influenced deeply by the First Amendment and strongly held beliefs about free expression. As we consider privacy law in Europe, we do so from an American perspective. Europeans similarly view American law from their own vantage point.

It is equally important to remember that technological changes that have occurred since 1995 have affected data protection in Europe — and every other privacy protection system — dramatically. Were the Centre to assess privacy protections in Canada, Australia or any other

established privacy regime, we would likely find limitations in those laws as well brought about by the evolution of technology.

I. Summary: While the EU Data Protection Directive (the Directive) is based on well-established and relevant principles of fair information practices, it applies them in a way that is not sufficiently flexible to promote the rapid innovation necessary for competitiveness and economic growth and to protect individual privacy.

Innovations in technology; rapid increases in data collection, analysis and use; and the global flow of and access to data have made an unprecedented array of products, resources and services available to consumers. These developments in no way diminish an individual's right to the secure, protected and appropriate collection and use of their information. Yet the manner in which those protections are provided is often challenged by the dynamic, increasingly international environment for information.

The principles of fair information practices upon which the European Directive is based remain respected, relevant and tested guidance for the appropriate use and protection of data.[1] But the global flow, innovative uses and market demands for data test the way in which the Directive applies those principles. In this environment, individuals maintain the right to secure and protected processing and storage of their data that does not compromise their privacy. At the same time, protection must now be sufficiently flexible to allow for rapidly changing technologies, business processes and consumer demand.

---

[1] The Privacy Act of 1974 95 U.S.C. Sec 552a and the Organization for Economic Cooperation and Development's "Guidelines on the Protection of Privacy and Transborder Data Flows" are also based on principles of fair information practices.
<http://www.oecd.org/document/18/0,3746,en_2649_34255_1815186_1_1_1_1,00&&en-USS_01DBC.html>

The European Commission's 2010 consultation on a possible reform of the Directive[2] recently signaled a growing recognition that some aspects of the EU approach are not optimal.[3] In some cases, the Directive imposes administrative requirements that do little to further privacy but that place significant burdens on companies — and on regulators. In others, the manner in which the Directive implements certain principles of fair information practices does not reflect the realities of the current data environment, and results in *pro forma* compliance that does not necessarily yield good privacy outcomes. Perhaps most significantly, the Directive is often perceived as impeding or slowing the global flow and sharing of data so necessary to innovation and international competitiveness.

In November 2010, the Commission released a communication that acknowledged that rapid technological developments and globalization have profoundly changed the data environment, and brought new challenges to data protection.[4] It noted the need to streamline and modernize the Directive, taking particular account of the challenges resulting from globalization and new technologies.

This testimony highlights key areas where the Directive is dated. It is not intended to be a complete analysis of European data protection law.

---

[2] Consultation on the Commission's Comprehensive Approach on Personal Data Protection in the European Union. < http://ec.europa.eu/justice/news/consulting_public/0006/com_2010_609_en.pdf>.

[3] In 2009, the European Commission launched a review of the current legal framework on data protection, starting with a high-level conference in May 2009, followed by a public consultation running until the end of 2009. Targeted stakeholders' consultations were organized throughout 2010.

[4] On November 4, 2010 the European Commission released a communication outlining its preliminary proposals to revise the EU Data Protection Directive (95/46/EC), entitled "Communication From the Commission to the European Parliament, the Council, the Economic and Social Committee and the committee of the Regions, A Comprehensive Strategy on Data Protection in the European Union." <http://ec.europa.eu/justice/news/consulting_public/0006/com_2010_609_en.pdf>.

II. The Directive imposes administrative notification requirements that often do little to advance privacy, but that place significant burdens on companies.

The Directive imposes on data controllers, *i.e.*, those persons responsible for data, the obligation to notify EU Member State data protection authorities of the processing of personal data.[5] Such notification is required when information systems are created and modified, and when personal data is transferred outside the European Union. This notification requirement increases the administrative burden on industry, enhancing neither the security of data nor the privacy of individuals. National data protection authorities must invest significant resources into managing and responding to this notification process.

Moreover, the Directive 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 transfer and, in some cases, obtain prior approval.[6] Such approval can easily take six months to obtain, and at the cost of significant resources for the company and the data protection authority.

Both organizations and regulators today are constrained by personnel and budget limitations. Complying with notification requirements diverts scarce company resources away from more productive activities that would enhance internal privacy programs and practices that would yield better privacy for consumers. Monitoring those notifications requires that regulators focus attention on good actors and away from companies that have demonstrated non-compliance and warrant close oversight.

---

[5] EU Directive, Article 18.

[6] EU Directive, Article 18 (e) and national data protection laws implementing this article.

It should be noted that the lack of harmonization across EU Member States exacerbates the burden of this requirement. Each of the 27 Member States' notification requirements differ to some extent from the others — sometimes in contradictory ways — and companies must comply with each.

III. Compliance with the Directive's requirement that organizations have a legal basis to process data does not always result in effective data protections or good privacy outcomes.

The Directive requires that organizations establish a legal basis for processing personal data,[7] and enumerates six criteria by which processing is determined to be legitimate.[8] The most significant of these criteria is informed consent of the data subject. To obtain such consent, companies must specify in their privacy policy the purpose for which the data will be processed. However, the ways in which data may be used evolve rapidly and may not be readily anticipated 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 to use data in unforeseen ways in the future. Such a requirement encourages instead creation of such broad privacy policies aimed at granting license to undertake any data activity companies see fit.[9]

---

[7] Under the provisions of the Directive, processing includes the act of initial collection of data. EU Directive, Article 2 (c).

[8] Criteria for making data processing legitimate include: 1) unambiguous consent by the data subject; 2) processing necessary to fulfillment of contract to which the data subject is a party; 3) processing necessary for compliance with a legal obligation to which the controller is subject; 4) processing necessary to protect the data subject's vital interests; 5) processing necessary to carry out a task in the public interest in the official authority vested in the controller or in a third party to whom data are disclosed; 6) processing necessary for purposes of the legitimate interests pursued by the controller or third party to whom data re disclosed, except where such interests are overridden by the interests of the fundamental rights and freedoms of the data subject. EU Directive, Article 7.

[9] Because the most important legal basis for processing is informed consent of the data subject, individuals will be put in the position to police the market against bad actors on the basis of their understanding of highly complex and broad notices.

IV. The Directive does not in many cases serve the global nature of data flows, and does not sufficiently take into account the way in which data is collected, used, stored, shared and accessed.

The global flow of data drives today's information economy. Innovation, efficiency and service depend on rapid and reliable access to data, irrespective of its location. Digital technologies and telecommunications and information networks provide seamless, low-cost access to data around the world. Remote storage and processing of data "in the cloud" dramatically change and greatly enhance the way individuals and organizations access information and software services.

The Directive's rules applying to the transfer of data to third countries do not work well in this emerging data ecosystem. They require that data only be transferred to countries that are found by the Commission to have attained status as providing "adequate" protections for personal data. Fewer than 10 countries have been found to be adequate.[10]

Other legal mechanisms are available to support the transfer of data under the terms of the Directive, but these are cumbersome.[11] The one flexible mechanism for data transfer from

---

[10] The European Commission has so far recognized Argentina, Canada, Faeroe Islands, Guernsey, Isle of Man, Jersey, the State of Israel, Switzerland and the US Department of Commerce's Safe Harbor Privacy Principles as providing adequate protection.

[11] Other legal mechanisms include unambiguous consent by the individual, participation in the U.S./EU Safe Harbor, transfer pursuant to fulfillment of a contract and model contracts for specific transfers. EU Directive, Article 7. Obtaining unambiguous consent is only possible when there is an equal relationship between the individual and the organization and cannot be used as the basis to transfer human resources data. EU/U.S. Safe Harbor is a bilateral process only available for transfers of data between the U.S. and the EU. Fulfillment of a contract is only available where the transfer of data is directly related to carrying out the terms of the contract. Model contracts must be reviewed and approved by the regulator and can take as long as six months to approve.

Europe is Binding Corporate Rules.[12] Gaining approval for BCRs is a lengthy and costly process, however, for both data protection agencies as well as companies, and does not scale to market demand.

The Directive also hinders the ability of organizations to engage in advanced processing activity such as analytics. Analytics involves an organization's broad analysis of data to determine what information the data itself can yield, its predictive value and whether it is sufficiently reliable that a company would act upon those findings. Analytics hold the potential to support powerful innovation, but the Directive's criteria for a legal basis for processing does not support their use.[13]

V. The Centre for Information Policy Leadership encourages consideration of alternative approaches to privacy and data protection that are based on fair information practices but that better reflect the realities of the evolving data environment.

The limitations of the Directive, as well as those of other regimes,[14] suggest that other approaches to privacy and data protection would provide more effective protections for

---

[12] Binding Corporate Rules (BCRs) were developed by the European Union Article 29 Working Party to allow multinational corporations, international organizations and groups of companies to make intra-organizational transfers of personal data across borders in compliance with EU data protection law. BCRs were developed as an alternative to the U.S./EU Safe Harbor (which is available to US organizations only) and the EU Model Contract Clauses. BCRs typically form an intra-corporate global privacy policy that satisfies EU requirements and may be available as an alternative means of authorizing transfers of personal data outside of Europe.

[13] Analytics represent another instance in which organizations may write broad and somewhat vague privacy policy notices to attempt to encompass a practice within the scope of the data subject's consent. See Section III.

[14] Japan undertook a review of its Personal Information Protection Act (PIPA) in 2006, one year after its enactment. Canada's periodic review of Personal Information Protection and Electronic Documents Act (PIPEDA) is currently underway. The Australia Law Reform Commission (ALRC) reported its findings about the need for change in that country's data protection law in 2008, and the government issued its response in 2009. Draft changes to the law were issued in 2010.

consumers and enhanced flexibility for organizations to make optimal, yet responsible, use of data.

Current discussions in the United States and in international forums have considered several approaches that hold great potential for achieving this goal. We encourage the committee to consider these as it continues its work on privacy protections in the United States.

An *accountability* approach has figured prominently in policy deliberations both in the United States and abroad. Accountability is characterized by its focus on setting privacy-protection goals for organizations based on criteria established in current public policy and on allowing organizations discretion in determining appropriate measures to reach those goals. An accountability approach enables organizations to adopt methods and practices to reach those goals in a manner that best serves their business models, technologies and the requirements of their customer. It relies upon credible assessment of the risks (assisted by, *inter alia,* the use of privacy impact assessments), the use of data may raise for individuals and responsible mitigation of those risks.[15]

The essential elements of accountability may be summarized as:

- Organization commitment to accountability and adoption of internal policies consistent with recognized external criteria.
- Mechanisms to put privacy policies into effect, including tools, training and education.
- Systems of internal ongoing oversight and assurance reviews, and external verification.
- Transparency and mechanisms for individual participation.

---

[15] This analysis is often referred to as one aspect of "privacy by design."

- Means for remediation and external enforcement.[16]

The Centre also encourages the committee to consider work currently underway on a *use-and-obligations* approach.[17] This model establishes the use rather than the collection of data as the primary driver of a data collector's obligations related to notice, choice, and access and correction. Under current implementation of fair information practices, consumer choice or consent to use data in certain ways establishes a company's responsibilities. A use-and-obligations model shifts responsibility for disciplined data use to the data collector and all holders of data, imposing requirements for transparency and notice, consumer choice, and access and correction on the data collector, based on the way the data is to be used.

The model takes into account all of the uses that may be required to fulfill the consumer's expectations and meet legal requirements. It imposes on organizations obligations based on five categories of data use: 1) fulfillment; 2) internal business operations; 3) marketing; 4) fraud prevention and authentication; and 5) external, national security and legal. It recognizes both aspects of a company's obligations, as articulated in fair information practices. The first includes the actions organization must take to facilitate individual participation — transparency (notice), choice, and access and correction. These ensure that an individual can know what data about him an organization is collecting or holds; can make choices about its use when practicable and

---

[16] For a comprehensive discussion of an accountability approach to privacy protection, see "Data Protection Accountability: The Essential Elements," October 2009, <http://www.ftc.gov/os/comments/privacyroundtable/544506-00059.pdf>; and "Demonstrating and Measuring Accountability: A Discussion Document," October 2010 <http://www.huntonfiles.com/files/webupload/CIPL_Accountability_Phase_II_Paris_Project.PDF>.

[17] The use-and-obligations approach is discussed fully in "A Use and Obligations Approach to Protecting Privacy: A Discussion Document," <http://www.huntonfiles.com/files/webupload/CIPL_Use_and_Obligations_White_Paper.pdf>.

appropriate; and can access and correct it in appropriate circumstances. The second includes the internal steps an organization takes to effectively manage data to minimize risk to both the organization and the individual — collection limitation and use minimization; data quality and integrity; data retention; security; and accountability.

VI. Conclusion

The limitations of the Directive discussed in this testimony highlight the challenges raised by advances in technology; innovative, complex business models; and the demand for nearly instantaneous movement of data around the globe. But in this rapidly evolving environment for data, notions of privacy remain based in local mores and cultures. Meeting the needs of the digital economy does not require countries to adopt each other's privacy values and approaches to protection, but to find ways to make those systems interoperable — respecting local privacy traditions while promoting the robust, protected flows of data necessary for a prosperity and economic growth.

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.

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:]

Written Statement of Professor Peter P. Swire
Moritz College of Law of the Ohio State University
Center for American Progress
Submitted to the House Energy & Commerce Committee
September 15, 2011
"Internet Privacy: The Impact and Burden of E.U. Regulation"

Chairman Upton, Ranking Member Waxman, and other distinguished members of the committee, thank you for inviting me to participate in this hearing on "Internet Regulation: The Impact and Burden of E.U. Regulation."

My testimony today makes three points:

First, the E.U. Data Protection Directive has deep roots in the United States approach to privacy. It incorporates the fair information practices that were first written in the U.S., and the Directive has most of the same elements as U.S. laws such as Gramm-Leach-Bliley and HIPAA. The privacy principles in Europe and the U.S. are thus quite similar, although our precise institutions for addressing privacy are different.

Second, support for basic privacy principles is good policy for the United States. A "we don't care about privacy" attitude from the United States would create major risks for American jobs, exports, and businesses. Other countries could then decide that the U.S. is a non-compliance zone, and ban transfers of data to the U.S. Foreign competitors could use the lack of U.S. privacy protections as a excuse for protectionism, and insist that information processing happen in their country, and not in the United States.

Third, in my book on the Directive and elsewhere, I have written criticisms of many aspects of European privacy law. With that said, the European regime has also made vital contributions to improving privacy practices in the U.S. and globally. Many of the sensible ways that we "self regulate" in the United States today depend on privacy good practices that were shaped by discussions in Europe about how to achieve business goals while also protecting individual privacy.

Background of the witness

I am the C. William O'Neill Professor of Law at the Moritz College of Law of the Ohio State University, and Senior Fellow at the Center for American Progress. In 1998 I was the lead author, with Robert Litan, of "None of Your Business: World Data Flows, Electronic Commerce, and the European Privacy Directive," published by the Brookings Institution. In 1999, after having previously led a U.S. delegation to Europe on privacy issues, I was named Chief Counselor for Privacy, in the U.S. Office of Management and Budget. In that role, I was the first (and thus far the only) person to have government-wide responsibility for privacy policy.

Among other activities in that position, I worked closely with the Department of Commerce in negotiation of the Safe Harbor agreement that the E.U. and U.S. signed in

2000. The Safe Harbor was negotiated because the Directive in many instances prohibits transfer of personal information to countries outside of the E.U. unless there is "adequate" privacy protection. Since 2000, companies that agree to comply with the Safe Harbor rules have been able to lawfully transfer personal information from the E.U. to the United States.

After working at OMB, in 2001 I returned to law teaching. I have written and spoken extensively on privacy and security issues, with publications and speeches available at www.peterswire.net. In 2009 and 2010 I was Special Assistant to the President for Economic Policy, serving in the National Economic Council under Lawrence Summers. In August of last year, I returned to law teaching for Ohio State. I live in the D.C. area.

American Roots of the E.U. Directive – Shared Privacy Principles in the U.S. and E.U.

In this hearing on the E.U. Data Protection Directive, it is useful to show the deep American roots for the Directive's approach to privacy, as well as major similarities in the principles of privacy protection shared by the U.S. and E.U. There are very important differences in the specific privacy rules and institutions, but the similarities are greater, in my experience, than many people are aware.

As the Committee knows, the "Fair Information Practices" ("FIPs") are a major foundation of privacy protection. These FIPs are built into the Directive, but the first publication of the FIPs came from the U.S. Department of Health, Education, and Welfare Advisory Committee on Automated Systems, in 1973. That Committee wrote:

"The Code of Fair Information Practices is based on five principles:

1. There must be no personal data record-keeping systems whose very existence is secret.
2. There must be a way for a person to find out what information about the person is in a record and how it is used.
3. There must be a way for a person to prevent information about the person that was obtained for one purpose from being used or made available for other purposes without the person's consent.
4. There must be a way for a person to correct or amend a record of identifiable information about the person.
5. Any organization creating, maintaining, using, or disseminating records of identifiable personal data must assure the reliability of the data for their intended use and must take precautions to prevent misuses of the data."

These FIPs were soon put into law in the United States. In 1974, Congress passed the Privacy Act, which continues to apply today for federal agencies. The Privacy Act contains legal guarantees for FIPs such as notice about the existence of systems of records, notice of what information is in those systems of records, choice about secondary use, access and correction of records, and reliability of data.

The FIPs and the Privacy Act had a profound effect on European data protection. Several key countries there passed their first data protection laws in the late 1970s and early 1980s. Also in this period, the Organization of Economic Cooperation and Development (OECD) promulgated its "Guidelines on the Protection of Privacy and Transborder Flows of Personal Data." These Guidelines adopt the FIPS. They are non-binding, but the United States was a leader in their drafting and the Guidelines have been a major source of subsequent privacy law worldwide. European privacy experts agree that these Guidelines were a key source for the E.U. Data Protection Directive.

The impact of these U.S.-originated FIPs has continued over time. The Federal Trade Commission, U.S. Department of Commerce, and other federal agencies have often has endorsed the FIPs. The Congress has included FIPs-style protections in numerous laws, including: Privacy Act of 1974; Family Educational Rights and Privacy Act of 1974; Right to Financial Privacy Act of 1978; Cable Communications Policy Act of 1984; Electronic Communications Privacy Act of 1986; Employee Polygraph Protection Act of 1988; Video Privacy Protection Act of 1988; Telephone Consumer Protection Act of 1991; Driver's Privacy Protection Act of 1994; Health Insurance Portability and Accountability Act of 1996; Children's Online Privacy Protection Act of 1998; Gramm-Leach-Bliley Act of 1999; CAN-SPAM Act of 2003; and Fair and Accurate Credit Transaction Act of 2003. This history shows that the American-originated FIPs have had a profound effect on privacy laws in Europe and globally, and are incorporated into many American laws today.

In the area of fundamental rights, there is also greater overlap on privacy than observers often recognize. In Europe, privacy is considered a fundamental human right under Article 8 of the European Convention on Human Rights, adopted in 1950. Article 8 is entitled "Right to Respect for Private and Family Life" and it provides: "Everyone has the right to respect for his private and family life, his home and his correspondence." In the United States, the word "privacy" does not appear in the Constitution. But the Constitution contains important protections for privacy. For instance, the Fourth Amendment guarantees the "right of the people to be secure in their persons, houses, papers, and effects" – language written long before Article 8 and a model for it. The Third Amendment protects against a major privacy violation – the quartering of soldiers in our homes. The Fifth Amendment rule against self-incrimination protects our having to reveal information about ourselves. More generally, the Constitution protects liberty. Alan Westin's classic 1967 book "Privacy and Freedom" shows the historical, practical, and theoretical reasons why personal privacy is an essential component of human liberty. Excessive intrusion by the state and society threatens freedom.

This history, in my view, shows a substantial overlap between the European and American approaches to privacy protection. The specific laws and institutions differ in important respects. The basic principles of respect for the individual's privacy, however, are importantly similar.

Privacy and Protectionism – The Risk to U.S. Jobs and Businesses

I believe that the United States response to European privacy rules should answer two questions: What will encourage U.S. jobs, exports, and business? And, how we do establish workable and reasonable privacy protections for American citizens? One major risk is that the E.U. and other countries will use the relative lack of U.S. privacy protections as an excuse for protectionism against U.S. companies that process personal information.

An important reason for writing the Brookings book in 1998 was because of the risk of a trade war between Europe and the U.S. on privacy and transborder data flows. The answer we worked out was the Safe Harbor agreement in 2000. U.S. companies that entered the Safe Harbor were assured of smooth business relations with Europe, under a privacy regime that clarified a number of important practical implementation problems. This Safe Harbor was approved by the E.U. as providing "adequate" privacy protection, so that personal information could be lawfully transferred to the United States.

Over a decade later, the risk of protectionism is growing again for transborder data flows. The European Union is in the midst of a major revision of the Directive, and the leaders in that effort are pushing for stricter privacy protections in important respects. In addition, important trading partners of the United States are increasingly adopting Europe-style privacy regimes. India's privacy law came into effect this year, with limits similar to Europe's. Mexico and a number of other Latin American countries have recently adopted or are in the process of adopting privacy laws, generally modeled on the law in Spain and the European Union.

As we saw with Europe in the 1990s, there are at least two significant threats to American interests if these privacy regimes determine that the U.S. does not have strong enough privacy protections. First, there can be a categorical decision that U.S. protections are not good enough – not "adequate" in the language of the Directive. Such a decision could affect entire industries. Second, the lack of U.S. privacy rules can become a powerful excuse for protectionism, risking U.S. jobs and the sales of U.S.-based businesses. Prior to the Safe Harbor, there was a widespread perception that American-based companies were subject to stricter privacy enforcement in Europe than domestic companies. The Safe Harbor created important safety for U.S.-based companies. The Safe Harbor does not exist, however, for India, Latin America, and other countries that have adopted privacy laws since 2000, including Japan and South Korea. It is also not clear whether the Safe Harbor would apply if and when the E.U. updates its Directive.

Cloud computing provides a vivid example of the risks to U.S.-based industry. Information services, including cloud computing, are an area of global leadership for the United States. The Province of British Columbia, however, a few years ago expressed concerns that U.S. privacy laws are not protective enough, and barred some contracts that would have sent data to the U.S. for processing. This year, there have been serious discussions in European legislatures that the Patriot Act and other features of U.S. privacy law make it too risky for the data of European citizens to be stored in the U.S.

U.S. Privacy Strategy in a World with National Enforcement

The cloud computing example illustrates the risk that local companies will use weak U.S. privacy laws as a reason to favor local industry, at the expense of U.S.-based companies. The challenges for the U.S. are greater because enforcement agencies in other countries have powerful tools at their disposal. For instance, just this week the German state of North Rhine-Westphalia announced a privacy fine of 60,000 Euros against a financial firm for improper affiliate sharing.

A "we don't care about privacy" attitude from the United States creates major risks for U.S. jobs, exports, and businesses. The risks apply for key areas of U.S. business strength, including cloud computing, information services, Internet sales, and other businesses that rely on using personal information. Privacy regulators in other countries can decide that the U.S. is a non-compliance zone, and ban transfers of data to the U.S. Foreign competitors can gleefully point to the lack of U.S. privacy protections, and insist that information processing happen in-country, and not be a service provided in the United States.

U.S. based companies cannot simply ignore the privacy regulators that exist in almost all of our major trading partners today. Many U.S. based companies have employees and assets in these countries. Those assets can be taken in privacy enforcement actions, and employees themselves are subject to strict penalties, as illustrated by the criminal penalty in Italy against a Google employee.

My view is that United States interests are served better by emphasizing our similarities on privacy rather than our differences. This approach was important in avoiding a trade war in the period leading up to the Safe Harbor agreement in 2000. The current Administration has taken this approach in the Commerce Department Green Paper on privacy, which supports basic privacy principles while cautioning against ill-considered regulations. The Federal Trade Commission, as an independent agency, continues to push for better privacy practices in the U.S., encouraging effective self-regulation but willing to see stricter rules go into place if industry does not safeguard information responsibly.

One example of this constructive approach has been the United States' participation in the annual Data Protection and Privacy Commissioners conference, held last year in Jerusalem and this fall in Mexico City. Historically, the United States was excluded from the official "closed" session, on the grounds that we did not have an independent Data Protection Authority such as exists in each European country. In 1999, when I served in the Office of Management of Budget, I was admitted to this session on "observer" status. In subsequent years, U.S. officials continued in that observer status. Last year, for the first time, the Federal Trade Commission was granted full membership in the closed session. The United States is thus at the table for key international meetings about privacy issues, and we are able to explain the American perspective and protect American interests. Over time, European and other privacy officials have gained a far greater appreciation for the substantial privacy protections that do exist in the United

States, including the numerous U.S. statutes listed earlier. The factual foundation created by this work, combined with current efforts by the Commerce Department and FTC, provides a potent response to the protectionist impulse that might otherwise block U.S. businesses.

In short, U.S. jobs, exports, and businesses benefit from a strategy that emphasizes our common privacy principles, and engages privacy regulators overseas in a way that minimizes the risk of their protectionist impulse. The United States will and should maintain its own privacy legal structure. But my experience is that members of Congress and the American people do believe in common-sense privacy protections, and we should emphasize that fact while avoiding overly-prescriptive regulations.

Strengths and Weaknesses of the E.U. Privacy Regime

As the sole minority witness in a hearing that emphasizes the "burdens" of the E.U. Directive, I believe it is helpful to include in the record some of the strengths of the European approach.

In the 1998 book on the Directive, written as it was going into effect, we wrote in detail about weaknesses in the European privacy regime. The example that perhaps got the most attention was the question of whether a person could legally take a laptop computer containing personal information from Heathrow Airport to the United States – whether that would count as an illegal transfer to the United States. One E.U. official said that this sort of laptop export could be a violation of the Directive. I believe this example helped focus attention on the practical problems in implementing the Directive.

As we have gained experience with the Directive since that time, it is worth noticing that the Directive has not interfered with business travellers and their laptops. The Directive has the flaw of appearing to prohibit a wide range of behavior, but common sense generally applies in daily activity. This "aspirational" model of law, where broad rights are stated in vague terms, is different from the typical American statute, which is more specific in describing requirements and exceptions. I remain concerned that European law often does not provide enough guidance to system owners about what exceptions exist and where compliance is actually required or not.

In the 1998 book and elsewhere, I have written about other concerns I have with the Directive. For instance, the Directive has a narrower view of free speech protection than the First Amendment provides in the U.S. I am also concerned about a worrisome tendency to expand the scope of what counts as personal data, in ways that could apply the Directive's regulatory apparatus to web logs and other essential components of the Internet.

There are also very important strengths in the European approach, which should be considered in any fair overall assessment of their system and ours. At the most general level, the Directive assures that there is a "cop on the beat." The Data Protection

Authorities give sustained institutional attention to privacy. These DPAs can address the constant stream of privacy issues created by evolving technologies.

The European DPAs also work together to study and engage on emerging privacy issues. Their role is described well in a letter this week by the Trans Atlantic Consumer Dialogue, which has been submitted to the Committee. That letter states:

"Seventh, the EU Data Directive also incorporates a structure to assess new challenges to privacy and to make appropriate recommendations following study and review. The Article 29 Data Protection Working Party, established by the Directive, has produced almost 200 reports and recommendations for the consideration by EU policymakers. The United States does not appear to have any comparable agency to meaningfully assess such topics as Geolocation services, the use of RFID in identity documents, cloud computing services, or data protection issues related to money laundering."[1]

In the United States, the Federal Trade Commission plays a similar role on some issues, but the breadth of engagement by the European agencies is greater than FTC staffing currently supports.

My experience in the privacy field for nearly twenty years leads me to the conclusion that the sustained engagement by Data Protection Authorities has had a major and often positive effect on the privacy practices of global companies. These practices, in time, spread to a wider range of organizations as best practices become standard practices.

A new privacy issue is often first raised publicly by a Data Protection Authority or the Article 29 Working Party. The issue is then often discussed by companies, technical experts, government officials, and privacy advocates. My view is that the outcome is often less strict and more practical than an initial reading of the Directive and national laws might seem to indicate. The outcome is often more protective of privacy than if the debate had not occurred. The practices that emerge from these discussions often become the norm for the industry.

One example of this pattern is the decision by major search engines (Google, Microsoft, Yahoo) to limit the time they would keep search history in identifiable form. The companies previous kept this data indefinitely in a form that could be easily linked to an individual. This basically meant that they were building up a lifetime record of each person's search history. After discussion with European authorities, as well as the FTC, the companies agreed to anonymize the search history after a number of months. This outcome, in my view, provided significant privacy protection – many of us would not want our search records from long ago to be potentially revealed to unknown persons. The outcome was also practical from a business point of view.

Another example of an idea from Europe that has spread is the Chief Privacy Officer. German law has long encouraged this approach. Many U.S. companies have CPOs today, CPOs exist in major federal agencies, and HIPAA requires covered entities

to have a designated person responsible for privacy. From an initial group of about 150 persons in 2001, the International Association of Privacy Professionals today has over 9,000 members, and it has credentialed thousands of Certified Information Privacy Professionals. These privacy professionals provide an institutional expertise that enables organizations to live up to the privacy and security promises they have made to individuals, both in the United States and abroad. Without such information experts in today's world of complex data flows, a company would often find it difficult to understand how to handle customer's data legally and appropriately.

This sort of dialogue, prompted in many cases by privacy officials in Europe, is a far cry from the caricature one sometimes hears of regulation-mad agencies bent on destroying commerce. Information technology and practices about information change rapidly. The European institutional commitment to privacy has undoubtedly deepened and broadened our understanding of these issues. Today, many sensible safeguards exist in the "self regulated" U.S. market at least in part due to the efforts of privacy officials in Europe.

In conclusion, I thank the Committee for asking me to testify here today, and I am glad to answer any questions you may have.

---

[1] http://tacd.org/index2.php?option=com_docman&task=doc_view&gid=329&Itemid=40

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. OK. 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 them.

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 are 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 OK—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. OK.

Mr. STEARNS. Amen.

Ms. TUCKER. Amen. OK. 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:]

FINANCIAL TIMES

May 25, 2011 10:25 pm

Companies in confusion over 'cookie' laws

By Maija Palmer, Technology Correspondent

Companies across Europe are in a state of confusion over what they need to do to comply with new internet privacy laws that come into force on Thursday.

The way that most companies currently collect information about people who visit their websites – using so-called "cookies" or small pieces of tracking code – will become illegal under the new European Union rules, and punishable in the UK, for example, with fines of up to £500,000 ($813,000).

Companies operating in the region must now get permission from web users for this kind of tracking, but there is little guidance on how they should do so.

Internet companies such as Facebook and Google are particularly concerned that the new laws could put their businesses in jeopardy, and advertisers are worried that the market for highly targeted internet advertising – worth nearly £100m a year in the UK alone – could be damaged.

The laws will touch every company that does business over a website. Any site that sells products or carries advertising will use cookies. Cookies can track items that a customer is putting into a website shopping basket, for example, or note the web pages individuals visit and send this information to advertising companies. Most websites will have between 10 to 20 cookies; big corporations with multiple websites could have hundreds or even thousands in use.

In the UK, the government issued three clarifications in the past two days, attempting to reassure companies that they will be given time to comply. The UK Information Commissioner's Office said it could give companies up to a year to change their websites.

However, Peter Gooch, privacy expert at Deloitte, said few companies had activated plans to change their websites.

"I haven't seen any of the big organisations outline a strategy of what they will do. They are playing the waiting game. If you stick your neck out with a solution and there is a bad

consumer reaction against it, it could be very damaging," he said.

"The guidelines produced by the ICO seem to pose more questions than answers," said Andreas Edler, managing director of Hostway, which provides internet services for a number of small business clients. "It still is unclear ... what changes users need to make in order to comply with the legislation."

Hiscox, the insurance company, has said it is concerned about the increased risk of litigation for the technology and marketing companies it insures.

"There is concern that companies can be fined or have a case brought against them by a group of individuals who feel their privacy has been violated," said Alan Thomas, head of technology and media at Hiscox.

Internet marketeers say getting permission from consumers to collect their data could be difficult.

"People are panicking a bit and wondering how this will mess up their analytics," said Dennis Dayman, chief privacy officer at Eloqua, a company which provides technology to marketing companies.

"Getting consent is difficult. As soon as you raise it people start to think there is something sinister in what you are doing. We are going to have to work on new ways of getting consent," said Ben Cooper, a director at Tullo Marshall Warren, the digital marketing agency.

Online privacy is becoming a growing issue for consumers. Large scale data loss incidents, such as the hacking attack on Sony's PlayStation Network, are making people increasingly question what details companies should collect and keep about them.

A test case may be needed before the law is clarified, Mr Cooper said. "There will be one or two high profile organisations that fall foul of the law. That will help test the boundaries."

Printed from: http://www.ft.com/cms/s/2/033a2568-86f4-11e0-92df-00144feabdc0.html

Print a single copy of this article for personal use. Contact us if you wish to print more to distribute to others.

© THE FINANCIAL TIMES LTD 2012 FT and 'Financial Times' are trademarks of The Financial Times Ltd.

FINANCIAL TIMES

June 21, 2011 6:00 pm

Dutch cookie law may lead to online exodus

By Matt Steinglass in Amsterdam

Web publishers have warned that a strict new internet privacy law set to be adopted in the Netherlands could cause them to shift some operations to other European countries.

The law, which the Dutch parliament is likely to approve on Wednesday, would force websites to ask users for specific permission before recording their personal data, or providing the data to third parties. It is part of a European Union-wide push to regulate user-tracking files known as "cookies".

The move is provoking controversy because of an amendment, approved on Tuesday by opposition parliamentarians, which requires websites to be able to prove that users have approved the use of their data.

Website developers and online advertisers warn the amendment will create headaches for developers, and could force users to click more pop-up windows while navigating the internet.

And because it will make the Dutch law stricter than those in Britain or France, they say it may lead to Netherlands-based web publishers shifting some operations elsewhere in the European Union.

The amendment is "a very hard-to-explain deviation from the European directive, which doesn't help anybody and makes it more complicated for both us and for the consumer," said Michiel Buitelaar, head of development at Sanoma Netherlands, the country's largest web publisher. "It's really very disappointing."

"We can't have this sort of splendid isolation in the Netherlands," said Afke Schaart, a member of parliament for the governing Liberal Party. "If something needs to be changed, it should be changed at the European level."

Parliament members who backed the amendment denied that it was out of step with the European directive. "We are simply taking into account the privacy interests of the internet user," said Kees Verhoeven of the left-liberal D66 party, which voted for the

measure.

Cookies are small text files that websites save on internet users' computers to record data about their browsing behaviour. Other websites can use cookie data for various purposes, such as sending personalised advertising.

The Dutch law implements a two-year-old EU internet privacy guideline, which member states were supposed to incorporate into their national legislation by May 25.

The Dutch government initially proposed that use of cookies be self-regulated by an existing industry standards board, the Advertising Code Commission. But parliamentarians found this arrangement too open to abuse, and an unlikely alliance of the far-right Party for Freedom of Geert Wilders and the leftwing opposition Labour Party proposed amendments requiring explicit user consent.

When lawyers and industry experts complained that the amendment failed to specify how often consent would be required or how it could be passed on to third parties, the measure was changed. It now explains that users should not "be asked to give permission every time a cookie is placed or read," but that whoever collects user data must have the user's permission to do so.

Industry experts say this direction is vague and will be difficult to implement. Neelie Kroes, the former Dutch transport minister and current European Commissioner for Digital Agenda, opposes the amendment.

But the amendment is now incorporated in revisions to the Telecommunications Law that are almost certain to be approved on Wednesday.

"We leave it up to the sector" to find a technical solution, said a D66 spokesman.

Printed from: http://www.ft.com/cms/s/2/7ee1f778-9c1f-11e0-acbc-00144feabdc0.html

Print a single copy of this article for personal use. Contact us if you wish to print more to distribute to others.

© THE FINANCIAL TIMES LTD 2012 FT and 'Financial Times' are trademarks of The Financial Times Ltd.

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:]

The Honorable Mary Bono Mack
Chair, Subcommittee on Commerce, Manufacturing and Trade
United States Congress
2125 Rayburn House Office Building,
Washington, DC 20515

The Honorable G.K. Butterfield
Ranking Member, Subcommittee on Commerce, Manufacturing and Trade
United States Congress
2125 Rayburn House Office Building,
Washington, DC 20515

September 14, 2011

Dear Chairwoman Bono Mack, Ranking Member Butterfield and Members of the House Subcommittee on Commerce, Manufacturing and Trade,

We are writing to you regarding the hearing entitled "Internet Privacy: The Impact and Burden of EU Regulation" scheduled for Thursday, September 15, 2011 on behalf of the Transatlantic Consumer Dialogue (TACD), a coalition of more than 80 consumer organizations in North America and Europe.[1]

We appreciate the interest of the United States Congress in the very important issue of Internet privacy. There are few issues of greater concern to Internet users in Europe and the United Stated today than the protection of personal information. [One has only to open a newspaper to read a report (mostly from the United States) about the loss of sensitive medical information, the mismanagement of security protocols at banking institutions, or the enormous cost that identity theft continues to impose on consumers and businesses.]

TACD is therefore somewhat surprised by what appears to be an effort to call into question the purpose and "burden" of the EU Data Directive. Given the widespread agreement across consumer organizations in both Europe and the United States that the United States lacks adequate privacy safeguards and that the US privacy laws lag woefully behind current technology and business practices, we expected a hearing that would focus on the lessons that the Congress might draw from the EU experience with data protection.[2]

---

[1] "The TACD is a forum of US and EU consumer organisations which develops and agrees on joint consumer policy recommendations to the US government and the European Union to promote the consumer interest in EU and US policy making." TACD, http://www.tacd.org/

[2] By way of example, the US federal wiretap law the Electronic Communications Privacy Act has only been updated twice in the past twenty-five years and both times to comply with law enforcement demands (the "CALEA of 1994" and the "PATRIOT Act of 2001.") None of the recent consumer privacy concerns, such as locational tracking, online advertising or mobile services, have been addressed in US federal law as they have been in European Union law.

TACD Secretariat, 24 Highbury Crescent, London N5 1RX, UK
Tel : (+44) 207 226 6663 Fax : (+44) 207 354 0607 email : tacd@consint.org Website : www.tacd.org

As it does not appear that your hearing plans to provide this perspective, we offer this letter and ask that it be entered in the hearing record so that the Members of Congress and their staffs might better understand the important role that the EU Data Directive, and the associated EU E-Privacy Directive, play in safeguarding the interests of consumers and businesses. We hope this will also lead to a substantive effort on the US side to address these issues.

First, as a matter of history, the EU Data Directive came about in the 1990s to streamline the European regulatory process and to encourage the growth of markets. As Europe moved to integrate its national economies and to promote trade across national borders, there was a clear recognition of the need to develop EU-wide directives that would promote the transfer of "good, services, labor, and capital." The EU Data Directive is one of many Directives adopted by the European Union to promote trade and commerce.

Second, the EU Data Directive seeks to protect fundamental human rights, the right to privacy, the right to protection of personal data and also the right to informational privacy, which is established as a Constitutional right in Article of the Charter of Fundamental Rights and Article 8 of the European Convention on Human Rights.

Third, the EU Data Directive is a concise statement of principles that make clear to business and consumers what their rights and obligations are. Unlike the extraordinarily complicated regulatory process that the United States tends to follow (the "HIPAA" rules are more than 1,500 pages), EU privacy law is reasonably straightforward relying on commonsense terms and not a lot of "legalese."

Fourth, the EU Data Directive is technologically neutral, focusing on the collection and use of personal information and not the specific technologies involved. As such it has weathered technologically change over the last two decades fairly well. By comparison, many of the US privacy laws, e.g. for "video rental records," seem very much out of date.

Fifth, the EU Data Directive seeks to make business practices more transparent so that consumers can make more informed decisions in the marketplace. This includes a legal requirement that companies disclose to consumers the actual information about them that is collected, and not simply a rudimentary "privacy policy." Without the ability to obtain this information, consumers cannot make meaningful decisions and markets cannot operate. The current US position on consumer access to information stifles both markets and innovation.

Sixth, the aim of the Directive is not to "burden" businesses but rather to ensure that businesses comply with basic privacy obligations that help ensure trust and confidence in the marketplace and facilitate the cross-border flow of data. Without such baseline standards, the risk of consumer revolt and market collapse is very real, as the U.S. experienced over the last several years in housing markets when it chose to remove safeguards that protected both consumers and businesses.

Seventh, the EU Data Directive also incorporates a structure to assess new challenges to privacy and to make appropriate recommendations following study and review. The Article 29 Data Protection Working Party, established by the Directive, has produced almost 200 reports and recommendations for the consideration by EU policymakers. The United States does not appear to have any comparable agency to meaningfully assess such topics as Geolocation services, the use of RFID in identity documents, cloud computing services, or data protection issues related to money laundering.[3]

Eighth, the EU Data Directive borrows much from the original formulation of privacy laws developed in the United States. Your "Fair Information Practices," which set out the rights and responsibilities for those

[3] "Justice – Data Protection – Documents Adopted by the Data Protection Working Party, "http://ec.europa.eu/justice/policies/privacy/workinggroup/wpdocs/2011_en.htm

who collect personal data, were established in your Privacy Act, your credit reporting laws, and your laws to protect the privacy of educational records before they were incorporated in the EU privacy laws. Europeans sometimes also refer to the privacy tort as "the American tort" because it was adopted in the United States before it was recognized in other countries.

There is much that US lawmakers could learn from a fair and balanced review of the EU Data Directive, just as the EU has learned much from the US experience. Certainly, the Directive needs improvement. Strengthening enforcement is critical as is extending the principles to law enforcement activity. Much of this work is already underway.

As organizations representing several hundred million consumers in North America and the United States, we believe there is great urgency in the need for the US Congress to address meaningfully the new challenges to privacy. We see in the United States spiraling levels of identity theft and security breaches. The US generates more spam (unsolicited commercial email) than any other country in the world and spends more money monitoring its own citizens than any other country in the world.

Certainly, there is much the United States could learn from other countries about how to address such challenges and the EU Data Directive provides a very good starting point.

TACD and its member organizations would be pleased to assist the Committee and the US Congress on these efforts.

Yours sincerely,

Julian Knott
TACD Head of Secretariat
On behalf of the TACD Steering Committee:

- Rhoda Karpatkin, **Consumers Union**
- Edmund Mierzwinski, **Public Interest Research Group**
- Robert Weissman, **Public Citizen**
- Jean Ann Fox, **Consumer Federation of America**
- Monique Goyens, **BEUC (The European Consumers' Organisation)**
- Benedicte Federspiel, **Danish Consumer Council**
- Conchy Martin Rey, **Spanish Confederation of Consumers and Users (CECU)**
- Breda Kutin, **Slovene Consumers' Association**

Cc: Chairman Fred Upton and Ranking Member Henry Waxman, Energy and Commerce Committee

Cc: Energy and Commerce Committee members

TACD Secretariat, 24 Highbury Crescent, London N5 1RX, UK
Tel : (+44) 207 226 6663 Fax : (+44) 207 354 0607 email : tacd@consint.org Website : www.tacd.org

Mrs. BONO MACK. And again, the hearing is now adjourned. Thank you all very much.

[Whereupon, at 12:40 p.m., the subcommittee was adjourned.]

○