

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 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 previously 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