Second Annual European Data Protection and Privacy Conference
CFK Keynote Address
Transatlantic Solutions for Data Privacy
December 6, 2011
9:25-9:50 AM

As I listened to Viviane Reding describe the view from the European Commission, it was clear that we share the common goal of protecting private information while also facilitating innovation, trade, and economic growth. As we work to strengthen individual protections, there are great challenges, but also immense opportunities for cooperation.

We are watching closely the European Commission's review of the European Privacy Directive. I am sure many of you are watching the Obama Administration's data privacy process closely as well.

The Administration will soon be releasing a white paper setting out its framework for protecting consumer data privacy and promoting innovation in the global digital economy. Last March, the Administration announced it supports consumer data privacy legislation to establish a comprehensive Bill of Rights as a baseline for consumer data privacy. The forthcoming white paper will spell out the content of the Bill of Rights and provide a roadmap for Congress and the Administration to put it into effect.

The Administration's privacy framework has four key pillars to strengthen the underlying foundation of privacy protections in the United States and reinforce trust that is essential to the digital economy.

The first pillar is the Consumer Privacy Bill of Rights, a set of principles to provide clear protections for consumers and greater certainty for businesses. These principles are based on well-known and globally-accepted Fair Information Practice Principles (FIPPs). But they are reframed as affirmative statements of rights to give consumers understandable guidance as to

what they can expect or demand from companies and how they can take responsibility for their information.

The FIPPs are also reframed to adapt to today's constantly evolving technologies by recognizing the incredible diversity of actors and ways in which people interact in the Internet environment. Notice and choice remain important elements of privacy protection, but the FIPPs provide a uniform set of standards and expectations for customers that expands on notice, and takes a broader, more interactive approach to effective privacy protection.

The Consumer Privacy Bill of Rights calls for a context-specific application of general principles to evolving technology platforms and business practices. It intends for companies to act as stewards of personal data by paying close, continuous attention to what consumers are likely to understand about their data practices based on the products and services they offer, how they explain their uses of personal data when delivering products and services to consumers, research on consumers' attitudes and understandings, and feedback from consumers. The less likely a consumer is to understand and anticipate that personal information is being collected or used, the greater the obligation of a company to provide notice and control to the consumer. By considering the perspective of the consumer and building a relationship with customers around privacy, companies will provide more effective consumer privacy protections, yet maintain flexibility to do so in ways that make sense for their business. Regulators should recognize that data use can offer enormous social as well as economic benefits, from free services to expanding frontiers of human knowledge; businesses should not be afraid to increase consumer awareness of these benefits.

We will ask Congress to enact the Bill of Rights to provide baseline consumer protections in those sectors not currently covered by legislation. But we will act to put the Bill of Rights into practice without waiting for legislation.

That brings me to the second pillar of the Administration's privacy framework: to convene multi-stakeholder processes designed to develop legally enforceable codes of conduct. Such codes of conduct will specify and expand upon how the principles set forth in the Consumer Privacy Bill of Rights apply in particular business contexts.

Multi-stakeholder organizations have played a major role in the design and governance of the Internet. They are uniquely responsible for its success. And they are essential to its future growth and innovation.

Even before privacy legislation is passed, the U.S. Department of Commerce will convene stakeholders to begin developing codes of conduct based on the Consumer Privacy Bill of Rights. Participation in the multi-stakeholder process will be voluntary, these forums will be open and transparent, and businesses ultimately will choose whether to adopt a given code of conduct. American businesses know, however, that once they commit to a code of conduct, their obligations for handling personal data become enforceable under law by the Federal Trade Commission (FTC).

We believe these processes will succeed because their openness, their inclusiveness, and their flexibility offer a win-win for businesses and consumers both. Traditional, top-down regulation moves at something far less than Internet speed and innovation. The multi-stakeholder process has proven the most capable model for addressing issues with the rapid, flexible, creative, and decentralized problem-solving required in the dynamic Internet environment.

The white paper will recognize that stakeholders include international partners. The processes we convene will benefit greatly from international participation. Codes of conduct developed with international stakeholders could lead to global consensus on privacy practices. They can supplement existing global frameworks, rather than supplant them, because multi-stakeholder processes can address emerging consumer privacy challenges rapidly and efficiently, far more than they could be addressed by legislation or regulation.

We invite your participation, and welcome your suggestions of issues to tackle.

The third pillar in our framework of enhanced consumer data privacy protection is effective enforcement. Privacy protections in the United States are effective because of vigorous law enforcement by the FTC and other agencies. No matter how strong or comprehensive privacy laws may be, they mean little unless they are enforced even-handedly. Companies must be held accountable for meeting not just baseline standards but for honoring the additional standards they adopt.

The Administration will urge Congress to provide the FTC and State Attorneys General with statutory authority to enforce the Consumer Privacy Bill of Rights. We urge the EU to take a similar approach to enforcing its privacy laws. The consistent and fair application of law to all companies, domestic and foreign, is essential to promoting international commerce.

The final pillar in the Administration's consumer data privacy framework — one I particularly want to emphasize today — is a commitment to increased global interoperability with the privacy frameworks of our international partners.

We have taken steps towards this goal for over ten years. When the EU passed its Data Protection Directive, the need for mechanisms to ensure that U.S. companies could keep doing business requiring data flows with firms in the EU produced the U.S.-EU Safe Harbor

Framework. We believed that companies seeking certainty under our laws would voluntarily subscribe to the Safe Harbor framework – and they have. Only four companies self-certified their compliance to the program when Safe Harbor was first launched, but today, nearly 3,000 companies of all sizes participate.

Safe Harbor is a valuable model of interoperability that has allowed cross border data flows to continue. And Safe Harbor also shows that once a company adopts a code of conduct, our FTC can enforce that code. The FTC has a history of pursuing companies that violate the Safe Harbor commitments. For example, in 2009, the FTC took action against six companies falsely claiming membership in Safe Harbor. More recently, in March 2011, the FTC alleged that when Google launched its social network, Google Buzz, it violated its Safe Harbor obligations, and recently settled these charges. Similarly, just last week, the FTC reached a settlement on charges that Facebook failed to comply with US-EU Safe Harbor commitments. Both Google and Facebook are now subject to independent privacy audits to monitor their compliance with Safe Harbor commitments for the next 20 years. These agreements now protect the millions of Europeans who use Google and Facebook.

The United States further demonstrated commitment to global interoperability with an international agreement among a number of Pacific nations. We participated in the development and adoption of the Asia Pacific Economic Cooperation's Cross Border Privacy Rules. The APEC rules promote accountability and enforcement across several Pacific nations; when they go live next year, they will help establish region-wide privacy policy compatibility that will lower costs of regulatory compliance and strengthen consumer protection across the region. We intend to continue our work with OECD and the International Conference of Data Protection and

Privacy Commissioners. I am not the first U.S. official involved in our privacy discussions to engage with all of you and I will not be the last.

In the forthcoming white paper, the Administration will recognize that although governments may take different approaches to privacy protection, it is critical to the continued growth of the digital economy that they strive to create interoperability between privacy regimes that often are fundamentally similar. The Bill of Rights articulated in the white paper is a strong step toward international consensus on privacy principles, and the white paper will underscore that increased interoperability requires international commitment to mutual recognition of each other's data privacy protection laws, an international role for multi-stakeholder processes and codes of conduct, and enforcement cooperation. Each of these components clearly will depend on close and continual engagement with our international partners.

As we work toward global interoperability, it is important that we have a discussion that is honest and fact-based.

To this end, let me say a few words about some of the differences between data privacy laws in the U.S. and in the E.U. I hope that the policy processes under way on each side of the Atlantic will narrow those differences.

But let us not overstate the differences.

I say this as someone who understands in a personal way some of the experience that informs European data privacy regimes. I bear some of the same scars: my mother was one of the refugees who streamed out of Paris in front of the Nazi occupation; her sister was interned by the Vichy Government for helping hide resistance fighters; the home my grandparents built in Brittany was requisitioned and later destroyed because it might give General Patton's army a spotting post; my great aunt and uncle were sent to Terezin, and records show, they went from

there “nach Östen” — to Birkenau; as a child, I lived in a divided Berlin still scarred by bombs, bullets, and fires.

Last year during the gathering of the International Association of Privacy Professionals, one data protection commissioner commented to me, “You know, a lot of my colleagues tell me Americans don’t care about privacy but, if that is the case, how come all the people who attend these conferences are American?” While our system does not have a law governing all commercial use of personal information — that is something the Obama Administration have set out to change — its protection of privacy is strong in practice.

This protection is rooted in values of individual autonomy and resistance to government intrusion into private life that are embedded in the U.S. Constitution and political culture. It is reinforced by the specific privacy laws for sectors such as health, finance, or education. For sectors not covered by a specific law, vigilant enforcement of general consumer protection laws by the FTC and State Attorneys General provide significant privacy protections. The FTC has broad power to regulate “unfair or deceptive acts or practices” and to hold companies accountable for the data protection promises they have made. Data breach laws in 46 states have added a powerful incentive to pay close attention to data privacy.

One misunderstanding I encounter relates to how so-called “self-regulatory” regimes operate in the United States. In the EU, privacy policies and company commitments generally are entirely voluntary and unenforceable absent a specific legislative obligation. In the U.S., a company that commits to a “self-regulatory” program or publishes a privacy policy faces FTC enforcement if these promises are broken. State Attorneys General may initiate similar enforcement actions. Our multi-stakeholder processes will incorporate this same force of law; in

my forward to the Department of Commerce Green Paper, I made it clear that "more than self-regulation is needed."

Another misunderstanding I often encounter is the misimpression that U.S. laws somehow give our law enforcement and national security agencies unfettered access to personal data. While the Administration's white paper focuses on commercial data protection, let me briefly address this issue.

This monster-under-the-bed was born of misconceptions about the USA PATRIOT Act and U.S. laws governing surveillance and access to electronic information. They are not based on actual comparison of the applicable laws in the United States and the E.U.

EU laws recognize that there are situations where law enforcement should have access to personal information subject to appropriate safeguards. So does U.S. law. But under the Electronic Communications Privacy Act and other U.S. laws, law enforcement and national security investigations are subject to significant constraints to protect individual privacy. The United States, along with 30 European countries, abides by the Cybercrime Convention, which sets forth the circumstances under which parties may compel production or conduct searches of computer data. Any companies that comply with lawful U.S. requests for information are acting in a manner consistent with the principles of the U.S.-EU Safe Harbor Agreement and the EU Data Protection Directive.

As Attorney General Eric Holder has observed, "[i]n the United States, our structure of government and the system of justice . . . reflect a core belief in the importance of protecting citizens from government intrusion. Our most important legal document – our Constitution – established a federal government with limited powers, and with extensive checks and balances; and our Bill of Rights ensures … freedom … from unreasonable searches and seizures. . . . Let

me be very frank and let me assure you today: Not only do the American people understand your concerns about, and commitment to, privacy rights – we also share them. That is why we have built robust privacy protections into our data collection programs – and that is why we will continue working to ensure that both privacy rights and public safety are protected."

To be clear, many of our European counterparts allow law enforcement access to electronic information in ways that would not meet the standards required by U.S. laws. To take just a few examples: in one of EU's largest member states, service providers may be ordered by district prosecutors to turn over files the prosecutors deem "relevant to the inquiry in progress." In another large member state, on similar grounds, a prosecutor may issue a search warrant for computer files. And in yet another state, a government agency is authorized – without a court order or any court review – to wiretap all telephone and Internet traffic that transits international borders. Such government actions raise significant privacy concerns beyond those implicated by U.S. law.

I understand DG Justice and our Justice Department plan an exchange in January on privacy and law enforcement, and that should help develop a fact-based comparison of what the laws actually provide and what law enforcement agencies actually do.

As the EU continues its review of the Privacy Directive, I urge you to consider changes that will provide strong consumer protections within a flexible framework that will facilitate the global free flow of information and trade.

Together, the United States and Europe have led the way to a global system of communications and trade on which our economies depend. The digital economy and society have transformed the way we provide services, purchase products from distant providers, and share information and ideas. The simple sharing of pictures between neighbors can implicate the

laws of multiple countries as data is transmitted over the Internet and stored remotely. Of course, in today's world, those images may come not from your neighbor, but from a student in Tahrir Square — and such images are transforming political debates across the world.

And, as these changes take place, some seek control of Internet traffic as a tool of social control and political repression.

At such a time, the United States and Europe should work in concert to prevent the building of more Great Firewalls. In developing data privacy rules in the United States and in Europe, let us act to preserve the model of free flow of information across borders that has made the Internet such a powerful tool of commerce, communication, and social organization. Let us provide frameworks for consumer data privacy that provide real and effective protections while enabling the growth, innovation, and free commerce that our economies need.

I want to thank Giles Merritt and Forum Europe for organizing today's conference. And I want to thank all of you for this opportunity to share my perspective on transatlantic cooperation for privacy protections. I look forward to working with you in upcoming multi-stakeholder processes and in more general discussions to improve global interoperability.