

International Association of Privacy Professionals (IAPP) Conference
CFK Keynote Address
March 9, 2012
12:15-12:30

It's great to be here today.

I was here yesterday and, as my staff and I were walking back into the office, someone asked "where are you coming from?" "We're coming back from IAPP," was the answer. "What's IAPP?" "The biggest gathering of privacy nerds you'll ever see." "Privacy nerds!? They're awesome!!"

That's how we think now at the Department of Commerce.

So — my fellow privacy nerds, distinguished guests, ladies and gentlemen ...

We meet at an important time for privacy both here in the U.S. and around the world.

For the first time, the President of the United States has called for legislation to provide every individual with baseline privacy protections as articulated in the Consumer Privacy Bill of Rights. President Obama said "[n]ever has privacy been more important than today, in the age of the Internet, the World Wide Web and smart phones," and his preface to the Administration's Privacy Blueprint is a ringing statement of a right to privacy deeply embedded in American values and American Law.

The President called on us in the Administration to advance the principles of the Privacy Blueprint, on Congress to enact legislation, and on "companies to begin immediately working with privacy advocates, consumer protection enforcement agencies, and others to implement these principles in enforceable codes of conduct."

This final statement of U.S. Government policy and legislative recommendation comes at the same time as the European Union is considering its own legislative proposal to modernize the 1995 Data Protection Directive.

In the Pacific region, members of the Asia-Pacific Economic Cooperation (APEC) endorsed the APEC Cross-Border Privacy Rules system in November, and this agreement is being implemented this year.

IAPP is a global organization. It's fitting that we have a global conversation about privacy. The Internet and digital technology have made the world smaller and more interconnected. We want to follow blog posts and tweets from Egypt and Syria. We expect our email to pop up nearly instantaneously without thinking about whether it crossed national

borders to get there. We demand information, goods, and services 24x7, whether they come from across town or from the other side of the world.

The discussions in the United States, the EU, and Asia are based on shared principles, shared commitment to the interoperability of privacy systems across borders, and a shared belief that sustaining consumer trust is essential to continued innovation and the growth in the digital economy in fragile economic times. People who have confidence that their privacy is respected are more likely to engage in political dialog, conduct commercial activity, and form social connections online.

As we turn to carrying out President Obama's direction to his Administration to advance the principles of Privacy Blueprint, we seek to bend the curve toward trust, certainty, and interoperability. In both what we do — the content of the Privacy Bill of Rights — and how we do it — the multistakeholder process to develop codes of conduct — we mean to be interactive, adaptive, and interconnected.

These are characteristics that have made the Internet and digital technology so revolutionary.

By reframing the Fair Information Practice Principles as an affirmative Bill of Rights in clear terms, we seek to inform and empower consumers with clear statements that spell out what they should expect. And we call on businesses to engage with consumers by looking at the principles of the Bill of Rights actively and holistically with a view toward acting as responsible stewards of data.

For too long, consumers and companies have lacked a consistent way to think about privacy. FIPPs may make sense to privacy professionals, but they are unintelligible to your average consumer. You can't have a conversation when only one side understands the language. And privacy needs to be a conversation.

No one principle can provide a complete roadmap. Notice and choice remain vital ingredients of privacy protection, but reliance on notice and choice alone can put form over substance. A more dynamic approach can strengthen the substance.

In particular, the Respect for Context principle refocuses use limitations from static provisions in privacy policies to an active inquiry into consumers' privacy expectations. The Focused Collection principle makes data minimization not an absolute but calls on companies to make considered judgments about what data they really need and why they need it.

The Privacy Blueprint calls for multistakeholder processes to begin — for businesses, consumer advocacy groups, academics, and other stakeholders to shape what the consumer privacy bill of rights means in specific contexts. We are moving forward: last week, NTIA sent

out a request for input on what issues the first multistakeholder processes should address, and what rules should govern specific processes. I encourage you all to participate, to make your voices heard in how to shape this process, to be early adopters of the privacy guidelines of the future, and to benefit from the consumer trust that will flow from commitments to follow these codes.

Now, many of you are corporate privacy officers. You may be asking what the multistakeholder process in the Privacy Blueprint means for you, what codes of conduct mean without enactment of legislation. Let me say to you — it is an opportunity.

Companies that are willing to engage in this process — to lead the way in adopting codes of conduct that make sense for the way business is done today, to implement the consumer privacy bill of rights applied to their sector or business model — will gain advantages.

They will be able to follow a road map that provides greater certainty that they are complying with consumer expectations and avoiding unfair or deceptive trade practices. More importantly, they will gain a competitive advantage over those companies that aren't willing to comply with a code of conduct. Those companies that subscribe to codes of conduct will send the message they want consumers' trust; those that don't subscribe will not.

Another major component of the blueprint is promoting international interoperability of privacy frameworks. We are moving forward on that front as well.

Last week, I traveled to Brussels, Berlin, and Munich for a number of productive conversations about the Privacy Blueprint and the Administration's plans with officials and stakeholders. The U.S. is preparing to participate in the APEC Cross-Border Privacy Rules. On March 19, the European Commission Directorate General will host our annual conference on the EU-US Safe Harbor Framework, which this year will also discuss more broadly where the US and EU are heading on data privacy.

There are differences in the Administration's blueprint for action and the European Commission's proposal, many of which are inherent in differences in our legal systems and not our understandings of privacy. We share many values, and the principles that underlie our respective frameworks are similar, including transparency, individual control, security, accountability, and access to personal data. EU Member States and the United States have long been committed to the privacy principles outlined in the 1980 Organization for Economic Cooperation and Development (OECD) Privacy Guidelines and, more recently, to the OECD Recommendation on Internet Policy Principles adopted last December.

Interoperability is not the same thing as uniformity. We will not erase differences — and we need not, because we have plenty of common ground for mutual recognition of our privacy frameworks.

Europe and Asia are vital trading partners. Mutual recognition is essential in the digital economy so that information — along with goods and services — can flow across borders. The APEC Cross Border Privacy Rules system will expand opportunities in the Asia-Pacific region. And for over 10 years, the US-EU Safe Harbor Framework has been a useful tool to protect consumer data while enabling companies to serve both sides of the Atlantic, and we look to its continuation.

The Administration remains committed to working with its partners in the EU and around the globe. And I look forward to working with my EU colleagues in March and beyond.

This is a remarkable time for privacy professionals — OK, privacy nerds — around the world. As President Obama said, “[o]ne thing should be clear, even though we live in a world in which we share personal information more freely than in the past, we must reject the conclusion that privacy is an outmoded value. It has been at the heart of our democracy from its inception, and we need it now more than ever.”

I am excited to be part of the Administration’s effort to protect consumer privacy and promote innovation in the digital economy. I am grateful to many of you here for the input and feedback you have provided us in that effort. I am more grateful still for the trust that so many seem willing to place in the Administration and the Department of Commerce, and in the process we have laid out.

We will work to keep that trust, with the understanding that you will join in the work of implementing the Consumer Privacy Bill of Rights in codes of conduct. Together, we will work out privacy rules for the 21st Century.