Data Protection & Privacy Regulation:
What impact on business and consumers?
Panel - The evolution in the approach to privacy:
The vision of US, EU and Italy
CFK Remarks
Thursday, 21 June 2012
11:00 am – 12:00 pm

The United States vision on privacy is expressed in the Consumer Privacy Blueprint released under President Obama's signature by the White House in February. It articulates a Consumer Privacy Bill of Rights and a policy framework for putting it into effect.

It also contains, in President Obama's preface, a stirring description of how privacy is deeply rooted in American values and embedded in American law -- enshrined within our bill of rights in the Fourth Amendment protection against government intrusion, and reflected early in our history by a law against intrusion on the US Mail.

Today, it is true, as some in Europe say, that we do not have "a law" on privacy; we have many laws on privacy. A Privacy Act from the 1970s that governs data in the hands of federal agencies. A cable television privacy law from the 1980s that governs cable subscriber records, and communications privacy laws for telephone, mobile, and video customers. A law to protect financial records, a law to protect the records of students at colleges and universities; as well as state laws such as data breach notification laws and common law protections; and strong enforcement by the Federal Trade Commission and State Attorneys General.

In 1973, in response to the rise of computerized data processing, the United States developed a Code of Fair Information Practices that created safeguards for how the government handled personal data. These Fair Information Practices became the basis of the FIPPs adopted and modified by the OECD, which in turn informs the 1995 European Privacy Directive and many other privacy frameworks.

These principles also are the starting point for the Obama Administration's Privacy Bill of Rights. which is a restatement of the FIPPs as an affirmative set of rights and expectations of a consumer, as opposed to the less-understandable listing of responsibilities of a data handler. The Administration's Blueprint calls for adoption of the Consumer Privacy Bill of Rights as binding law. We are in the process of drafting legislative text, and will work with the Congress to adopt a law that would provide the privacy protections stated in the Privacy Bill of Rights as a baseline and encourage industry to develop sector specific codes of conduct that implement these privacy protections.

As the Administration develops legislation, I am guided by three premises that recognize that in the digital arena, technology moves fast and that we want to encourage continued dynamic innovation.

The first is that governments are good at establishing policy objectives – such as ensuring consumers have adequate notice and control of their personal data – but are bad at knowing what is the best technology, standard, or method for achieving such objectives. When governments dictate a particular standard or technology, innovation is stifled and often the mandate becomes more of an obstacle to the policy than a solution.

Consider, for example, the policy objective of making cell phones more accessible for people with vision impairments. A decade ago, the way to accomplish this was to put a "bump" on the number five of a keypad. In the U.S., some advocated for such bumps to be required on all cell phones. If regulators had agreed, devices such as the iPhone might never been introduced.

The rapid pace of technological development nearly guarantees that the moment a protection is tied to a particular technology, it will be outdated. How long does it take to overhaul privacy regulations? The 1995 EU directive went into effect 3 years later, in 1998. The review of the privacy directive that began in May 2009 will result in changes taking effect perhaps in 2013, four years later? Is your source of news, the way you share information with friends and family, the websites you go to, your mobile phone, the same as it was four years ago?

In this space, government prescription is a prescription for failure, because solutions will lag behind technology, and therefore never provide effective privacy protections. And that is our goal – truly effective privacy protections for individuals.

Our second principle is central, and that is a focus on the multistakeholder process to incorporate the private sector, civil society, and other interested viewpoints into our policy. Our Privacy Blueprint also specifically notes that international parties are stakeholders in our process.

These processes are patterned on the way that we develop technical standards and the way that public-private partnerships like the Worldwide Web Forum have governed the Internet. A premise of this work is that this kind of public -private, transnational governance has been essential to the dynamism and growth of the digital economy and is essential to its future vitality.

The first multistakeholder process to implement the Privacy Blueprint is being convened by the National Telecommunications and Information Administration of the Department of Commerce to focus on transparency for mobile applications – how should companies providing applications and interactive services for mobile devices provide information to end users about how personal data is treated? Even the topic of this multistakeholder process was chosen carefully considering comments provided by a broad array of stakeholders across government,

commercial, civil society, and academic sectors. The first meeting will be in the Washington, DC area on July 12, 2012 and will be webcast. We have invited the European Commission to participate as an observer.

For us, multistakeholder processes are the key to the development of nimble and adaptive protections that incorporate the interests and concerns of consumers and businesses alike. This goes hand in hand with focusing on results, not methods.

The third key to ensuring that privacy frameworks provide real protections to individuals is effective enforcement and accountability. The best theory in the world is useless if it can't be put into practice and isn't followed on a day-to-day-basis. In the United States, we have strong enforcement by the Federal Trade Commission and by the state attorneys general. They can hold all companies accountable to the public commitments they make for handling personal data, via their privacy policy, by ascribing to Safe Harbor, or through any promise.

The same will apply to codes of conduct companies adopt through our multistakeholder processes. This is not simply self-regulation – as some people mistakenly believe– because this is a powerful enforcement tool. In the United States, these commitments are actively enforced by state and federal authorities, and have led, for example, to 20 years of privacy auditing at the risk of significant fines for some of the largest communications players in the world, including Google, Facebook, and Twitter. These companies are being held to commitments they created in a self-regulatory way by ascribing to Safe Harbor.

As we move forward with privacy policy legislation on both sides of the Atlantic, it is vital that we focus on making our systems interoperable. Interoperability does not mean the same. The US will not adopt the European system of data privacy, nor will the EU adopt a common law system. But our systems can be interoperable if the differences do not matter.

And they should not matter. The United States and European Union share common values. We share common principles on privacy. We have different ways of going about protecting privacy, but we both believe strong protections should be in place.

It is especially important in these challenging economic times. As Italy and the United States and European Union labor to reignite economic growth, we cannot afford to throw sand in the gears of the Internet. The US-EU trading relationship is the largest in the world and it is our longest standing one. More and more, that relationship depends on the exchange of data across national borders.

We need each other. So, as we move forward on privacy policy, let us focus on what we have in common. We have too much at stake to do otherwise.

Thank you very much.