Commissioner Julie Brill
Federal Trade Commission
EU Conference: Privacy and Protection of Personal Data
Keynote Address
March 19, 2012

Good afternoon. I am so delighted to be here.

Thank you to Vice President Reding and the European Commission for organizing this important event today. I know that DG Justice, led by Francoise Le Bail, has put considerable effort into this event—and it certainly shows.

This conference brings together many esteemed colleagues from the European Union and the United States—not only government officials, but also representatives from industry, academia and civil society.

We live in interesting times. When it comes to protecting consumer privacy, I can confidently say, and I am sure many of you can agree, we are at a pivotal moment.

The European Commission's proposed reform of the EU data protection framework,[1] the U.S. Administration White Paper,[2] and the very-soon-to-be-released FTC final privacy framework will be moving us all forward as we continue to work towards better protecting consumer privacy and contributing to the global privacy dialogue.[3]

We often hear about the differences between the U.S. and EU approaches to privacy. Many of these differences have been discussed throughout the day.

But it is worth focusing on the common ground—the baseline principles and ideas that are being discussed and implemented on both sides of the Atlantic.

We are at a moment when we all have a unique opportunity—and responsibility—to shape the future of privacy for the global community. Through these baseline principles, together we are calling on industry to:

---

[1] *See* Proposal for a Regulation of the European Parliament and of the Council on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data (General Data Protection Regulation) (Jan. 25, 2012), *available at* *http://ec.europa.eu/justice/data-protection/document/review2012/com_2012_11_en.pdf*.

[2] *See* Consumer Data Privacy in a Networked World: A Framework for Protecting Privacy and Promoting Innovation in the Global Digital Economy(Feb. 23, 2012), *available at* http://www.whitehouse.gov/sites/default/files/privacy-final.pdf.

[3] *See* A Preliminary FTC Staff Report on Protecting Consumer Privacy in an Era of Rapid Change: A Proposed Framework for Businesses and Policymakers (Dec. 1, 2010), *available at* http://www.ftc.gov/os/2010/12/101201privacyreport.pdf.

- Build privacy protections into your products and services through Privacy by Design.

- Provide more transparency so that consumers can better understand companies' collection, use and retention practices with respect to consumer information.

- Give consumers more effective tools to assert greater control over their information and how it is used.

- Provide appropriate access to the data companies hold about them.

- Take appropriate steps to ensure that the data they hold about consumers is accurate.

- Take reasonable steps to secure the data about consumers that they have.

- Give parents control over the information companies collect about their young children.

- And create a climate of accountability.

These commonalities show that both sides of the Atlantic are converging on key basic, important privacy principles.

As we think about our common principles as well as our differences, two important issues arise:

The first issue is whether we are doing a good job protecting our common principles through strong enforcement mechanisms.
And the second issue is whether, despite our differing privacy frameworks, businesses can effectively operate across borders.

Let me first talk about enforcement.

At the Federal Trade Commission, enforcement of existing privacy laws is "mission critical." We have challenged privacy and data security practices, and have brought enforcement actions, in a wide variety of sectors. We have brought cases in the social media space and in connection with behavioral advertising. We've sued companies spamming consumers and installing spyware on their computers. We've challenged companies that failed to properly secure personal consumer information. We have vigorously enforced the Children's Online Privacy Protection Act—the law designed to protect personal information about children.[4] And with the world moving to mobile, we have sued app developers who are not providing adequate information to consumers about their data collection practices. And we have warned other app

[4] Children's Online Privacy Protection Act of 1998, 15 U.S.C. §§ 6501-6506 (1998).

developers that their data collection and use practices may fall under the rigorous disclosure and access rules established under our Fair Credit Reporting Act.[5]

Our enforcement actions protect not only U.S. consumers, but the global community. The FTC consent orders arising from Facebook's "bunch of mistakes" and the launch of Google Buzz now protect more than the billion global consumers using the services of these companies.

The FTC's complaint against Facebook alleges a number of deceptive and unfair practices in violation of Section 5 of the FTC Act. [6]

And as you all know, we alleged that the company misrepresented its compliance with the Safe Harbor Framework.

The proposed FTC settlement with Facebook prohibits the company from misrepresenting the privacy and security settings it provides to consumers. Facebook must also obtain users' affirmative express consent before sharing their information in a way that exceeds their privacy settings. And when a consumer deletes his or her account or certain information from it, Facebook must block access to it.

Perhaps most significantly, we also require Facebook to implement a comprehensive privacy program that an independent auditor will monitor for 20 years. And we order Facebook not to misrepresent its compliance with the Safe Harbor Framework.

The FTC's consent order with Google also places similarly far reaching requirements on Google. [7] As in our Facebook settlement, the Google settlement requires the company to implement a comprehensive privacy program that an independent auditor will monitor for 20 years, and it orders Google not to misrepresent its compliance with the Safe Harbor.

Actions taken by the FTC in its headquarters just a cab ride away from here or considering the weather today, a nice walk have global implications. And that's the way it should be. In the Internet era, the enforcement actions of one regulator will often impact consumers in other parts of the world. This is more than Secretary of State Hillary Clinton's famous adage "it takes a village". It takes the global privacy enforcement community to provide effective consumer privacy protection in this increasingly interconnected world.

To that end, the FTC has worked hard to foster greater privacy enforcement cooperation. In 2010, the FTC, together with other data protection authorities, including a number from the EU, launched GPEN—the Global Privacy Enforcement Network—to foster cross-border cooperation among privacy authorities. And within other organizations, including the

[5] 15 U.S.C. § 1681s(a)(2)(A).

[6] *In the Matter of Facebook, Inc., a corporation* FTC File No. 0923184 (2011).

[7] *Google Inc., a corporation* FTC Docket No. C-4336 (Oct. 24, 2011) (Consent order). *Available at http://www.ftc.gov/opa/2011/10/buzz.shtm.*

International Conference of Data Protection and Privacy Commissioners, the FTC is working on fostering greater privacy enforcement cooperation.

The importance of international enforcement cooperation on privacy matters brings me to the second issue surrounding our commonalities and differences—the inter-operability of privacy frameworks. One measure of inter-operability is the extent to which our different frameworks allow for cross-border cooperation on enforcement matters. It is critical that privacy frameworks do not impede regulators from exchanging the information they need in order to pursue cross-border investigation of possible privacy and data security violations.

Of course, interoperability involves much more than the ability to cooperate on enforcement matters. It also requires the mutual recognition of privacy principles. And it means appropriate enforcement mechanisms for these protections. The Safe Harbor framework creates such interoperability between the E.U. and the U.S.

The APEC Cross Border Privacy Rules system is another example. In that system, an enforceable code of conduct is the basis for interoperability between different yet effective privacy regimes for purposes of cross-border data transfers.

The privacy frameworks being developed in both the US and the EU feature codes of conduct for industry to follow. As a 20-year plus veteran of law enforcement, my instinctual reaction to codes of conduct is this: meaningful enforcement mechanisms are critical in order for a code of conduct to be worth the paper it is written on, or the screen or smartphone you're reading it on.

Again, I thank my friends from Brussels for inviting me today.