Commissioner Julie Brill
German-American Data Protection Day
Consumer Privacy: U.S. Federal Trade Commission Recommendations for Businesses and Policymakers
May 10, 2012

Thank you for that kind introduction. It is wonderful to be here in Munich. My only regret is that my time in this wonderful city is very short. I had to choose between attending this event today and visiting the Hofbräuhaus. I'll need to come back to tour this beautiful city and include a visit there. Also I am terribly sorry I will miss the upcoming soccer final. I'm a huge futbol fan. Go Bayern München!

I have had the opportunity to meet with quite a few representatives from the German government during my two years as Commissioner of the Federal Trade Commission. I've spoken with German government representatives not only on a bilateral basis, but also within our dialogue with the European Union. In all of these contexts, I have engaged in many conversations about the importance of protecting consumers from privacy violations. Indeed, since I began as a Commissioner at the Federal Trade Commission, one of my highest priorities has been our agency's continued constructive engagement with our colleagues in the EU. It is opportunities like this one today that I value so highly, because they allow us to continue an important dialogue as we all endeavor to ensure that the personal information of consumers is protected as they navigate online, and increasingly, in the mobile space.

So much of our daily lives is now conducted on our laptops or in the palm of our hands on a mobile device, providing information, connection with friends and family, services and products, all at internet speed. But these benefits do not come without risks. In the United States, and in other parts of the world, we have been examining the need to better protect the collection and use of personal information of consumers. The question then becomes: how do we effectively protect the privacy of individuals and their personal information, while at the same time, enable industry to continue to innovate and delight us with the products and services that provide consumers with such important benefits?

Just six weeks ago, the U.S. Federal Trade Commission issued a report that aims to answer this question. The report sets forth our new framework on privacy.[1] It is the culmination of a process that included public forums and extensive input from industry, academics, consumer groups, technologists, and regulators both in the United States and abroad. Our final framework is intended to articulate best practices for companies that collect and use consumer information. These best practices can be useful to companies as they operationalize privacy and data security practices within their businesses.

The report also includes the FTC's call on the United States Congress to enact baseline privacy legislation, which will provide businesses with certainty and clear rules of the road, and will enable industry to act decisively as it continues to innovate.

[1] Protecting Consumer Privacy in an Era of Rapid Change: Recommendations for Businesses and Policymakers, An FTC Report (Mar. 26, 2012) *available at* http://www.ftc.gov/os/2012/03/120326privacyreport.pdf.

There are three main components to the final framework. First, we call for companies to build privacy and security protections into new products. Privacy and security simply cannot be an afterthought. Companies should consider privacy and data security at the outset, as they develop new products and services. This concept is often referred to as "Privacy by Design."

Second, we call for simplified choice for consumers. Consumers should be given clear and simple choices, and should have the ability to make decisions about their information at a relevant time and context.

Third, we call for greater transparency. Companies should provide more information about how they collect and use the personal information about consumers.

In an effort to promote simplified choice—the second component of the report—we called on industry to develop a Do Not Track mechanism that would enable consumers to make certain choices with regard to being tracked online across websites. And industry has made considerable progress here:

- by developing browser tools and icon-and-cookie based mechanisms for consumers to use;
- by promising to make these mechanisms interoperable by honoring consumers' choices no matter the mechanism through which consumers make their choices known; and
- by working to develop technical industry-wide standards to implement Do Not Track.

Do Not Track has the potential to provide consumers with simple and clear information about online data collection and use practices, and to allow consumers to make choices in connection with those practices.

Working with the various stakeholders who are developing an easy to use, persistent and effective Do Not Track system is one of the priorities that we at the US Federal Trade Commission will pursue over the next year as we implement the recommendations in the privacy report.

Our second priority involves the mobile space. The US Federal Trade Commission wants companies providing mobile services to work toward improved privacy protections, including the development of short, meaningful disclosures. Some sectors of the mobile industry are lagging in this regard: our recent survey of mobile apps for kids showed that very few provide information about how they collect, use and retain information about kids using their apps.[2] Industry must do better here. We will do our part as well: we plan to update our business guidance about online advertising disclosures and mobile disclosures. At a workshop at the end of this month, stakeholders will be able to provide us information about how to make mobile

[2] *See* Mobile Apps for Kids: Current Privacy Disclosures are Dis*app*ointing (Feb. 16, 2012) *available at:* http://www.ftc.gov/os/2012/02/120216mobile_apps_kids.pdf.

privacy disclosures short, effective, and accessible to consumers on small screens.[3] The Commission hopes that the workshop will spur further industry self-regulation in this area.

Another priority over the next year will be large platform providers, such as Internet Service Providers, operating systems, browsers, and social media. These large platform providers have the ability to track virtually all of a consumer's online activities. The Commission recognizes the heightened privacy concerns in connection with such comprehensive tracking. We believe that, at a minimum, heightened protection through robust notice and choice should apply to any entity that tracks virtually all of a consumer's online activities, whether through an ISP, operating system or a browser. In the coming year we will further explore privacy and other issues related to the potential comprehensive tracking that could be employed by ISPs, operating systems, social media, mobile browsers and other large platform providers.

Another priority for the FTC will be participating in the U.S. Department of Commerce's project to facilitate the development of sector-specific codes of conduct as articulated in the recent Administration White Paper on privacy.[4] As you may know, in February, the White House issued a report on privacy that included, as one of its main recommendations, the development of codes of conduct relating to privacy and personal information for industry sectors. The Administration's White Paper also recognizes the important role that the FTC will play in enforcing any codes of conduct that come out of the multi-stakeholder process.

While policy work, like the development of this final privacy framework, is a large part of the Federal Trade Commission's agenda, the agency is, first and foremost, a law enforcement agency. Two of the agency's most recent cases are important milestones in our enforcement work. These cases – against the Internet giants Google and Facebook – will play an important role in protecting consumers both here in Germany and around the world. We estimate that together, Google and Facebook have more than one billion users worldwide.

To ensure there is no misunderstanding, we examine companies' practices involving collection and use of consumers' information under Section 5 of the FTC Act, which prohibits unfair and deceptive acts and practices in commerce. It was intended to be broad, expansive and able to take into account changing practices and technologies, and was crafted by none other than Louis Brandeis.

The Federal Trade Commission charged Google with deceiving consumers when it launched its first social network product, Google Buzz.[5] We believed that Google took previously private information—the frequent contacts of Gmail users—and made it public in

---

[3] *See* Press Release, FTC, FTC Will Host Public Workshop to Explore Advertising Disclosures in Online and Mobile Media on May 30, 2012 (Feb. 29, 2012), *available at* http://www.ftc.gov/opa/2012/02/dotcom.shtm.

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

[5] *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.*

order to populate Google Buzz, all without the users' consent and in contravention of Google's privacy policy. The consent order settling this case requires Google to protect the privacy of consumers who use Gmail as well as Google's many other products and services. Now, if Google changes a product or service in a way that makes consumer information more widely available to third parties, it must seek users' affirmative express consent to such a change. And we imported into the Google consent order one of the most effective provisions in our many data security cases: these consent orders frequently include a requirement that the company develops and maintains a comprehensive data security program that is audited for 20 years. In the Google order, we require Google to implement a comprehensive privacy program and obtain independent privacy audits every other year for the next 20 years.

The Commission also believed that Facebook had engaged in a number of deceptive and unfair practices.[6] These include the 2009 changes made by Facebook so that information users had designated private – such as their "Friends List" or pages that they had "liked"—became public. The complaint also charged that Facebook made inaccurate and misleading disclosures relating to how much information apps operating on the site could access about users. For example, Facebook told users that the apps on its site would only have access to the information those apps "needed to operate." But we believed that apps could view nearly all of the users' information, regardless of whether that information was "needed" for the app's functionality. We also claimed that Facebook made promises that it failed to keep: it told users it would not share information with advertisers, and then it did; and it agreed to make inaccessible the photos and videos of users who had deleted their accounts, and then it did not.

Like the Google order, the Facebook order requires Facebook to obtain users' affirmative express consent before sharing their information in a way that exceeds their privacy settings. An important additional requirement, not present in the Google order because the facts didn't lend themselves to addressing this issue: Facebook must ensure that it will stop providing access to information after a user deletes it. But like the Google order, the Facebook order requires Facebook to implement a comprehensive privacy program and obtain outside audits for 20 years.

And just two days ago, the FTC announced another enforcement action involving another major social networking site—MySpace.[7] The FTC was concerned that, despite promising its users that it would not share consumers' personal information with advertisers, MySpace provided advertisers with the "Friend ID" of users who were viewing particular pages on the site. With the Friend ID, the advertiser could then locate the user's MySpace personal profile to obtain his or her real name and other personal information. Like Facebook and Google, if approved, the MySpace order would require the company to create a comprehensive privacy program and undergo third-party audits for the next 20 years.

Notably, Facebook, Google, and MySpace are participants in the U.S.-E.U. Safe Harbor Framework. An important part of the FTC cases against these companies was our allegation that each of them failed to live up to their obligations under the Safe Harbor. Now, as a result of our

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

[7] *In the Matter of Myspace LLC* File No. 102 3058 (May 8, 2012).

enforcement actions, all three companies – Google, Facebook and MySpace – are required to comply with the Safe Harbor, and they will be subject to penalties if they don't. The FTC is committed to the important role we play in enforcing the Safe Harbor Framework, and our recent enforcement work in this area demonstrates our seriousness about this commitment.

That leads me to the important issue of how we deal with cross-border privacy issues. As you know, the Safe Harbor Framework is a mechanism that facilitates cross-border data transfers from the E.U. to the United States. As both the United States and Europe have been examining privacy frameworks, one of the areas that we have both been considering is how different privacy frameworks can be inter-operable. By "inter-operable," I am referring to systems that, while they may not be the same, allow for mutual recognition and thus transfers of data across borders.

In order to create interoperability, we need a certain degree of commonality and shared privacy values. We hear so much about the differences between the E.U. and the U.S. approach to privacy. And I think we need to be mindful of these differences. But there is a commonality on key concepts and a considerable number of shared values. The question to ask then is: despite our differences, can we move towards inter-operability based on commonalities? I believe that the answer is "yes."

The Safe Harbor is one such mechanism that allows for inter-operability between the United States and the E.U. Another example of an inter-operability mechanism—one that is multilateral—is the APEC Cross Border Privacy Rules system. That system, which is currently in its final implementation phase, includes a set of detailed privacy requirements negotiated by the relevant stakeholders and authorities in the Asia Pacific Economic Cooperation Forum region based on the APEC Privacy Principles. These principles reflect a consensus among the APEC economies on what constitutes valid and sound privacy protection for cross-border data flows within the APEC region. In the APEC Cross-Border Privacy Rules model, businesses voluntarily agree to participate in this system, but once they have made that commitment, the privacy and data security requirements then become binding and enforceable against them.

Enforceable codes are now also featured in the new privacy models in the United States and in the E.U. The 1995 E.U. Data Protection Directive[8] allows for the development of codes of conduct, and it appears that under the new E.U. data protection proposal,[9] such codes of conduct may also have a role to play in cross border data transfers. Of course, Binding Corporate Rules already play a role in allowing such cross border data transfers. I understand there's an effort underway to examine the potential for inter-operability between E.U. approved Binding Corporate Rules and APEC Cross-Border Privacy Rules. And as I mentioned earlier, in the

[8] Directive 95/46, of the European Parliament and of the Council of 24 October 1995 on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data Directive 23/11/EC, 1995 O.J. (L 281) 31, 50.

[9] 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), Com (2012) 11 final (Jan. 25, 2012)

United States, the Department of Commerce will be working to develop industry codes of conduct that will hopefully lend themselves to cross-border application–that is certainly something that I believe we should aim for.

I'd like to end with this request: As we update and modernize our domestic privacy regimes on both sides of the Atlantic and everywhere else in the world, let's do so with inter-operability—that is, mutual recognition that allows for cross-border data transfers—in mind. Our modern global economy depends on the free-flow of data across national borders and thus requires interoperability and cooperation. Different privacy and legal regimes must work together—both on the level of substantive privacy protections and with respect to enforcement. Working with the models I just described, this goal is achievable.

Thank you again for organizing this event and for inviting me to speak today.