Practising Law Institute
Privacy and Data Security Law Institute
July 19, 2011

Good afternoon. It has been a full day here in the windy city and I am delighted to see so many of you at this session. I would like to thank the Practising Law Institute for inviting me to share my thoughts on privacy and data security with you today.

Privacy and data security fit comfortably within the Federal Trade Commission's larger mission of protecting consumers, whether it be from a merger that will lead to higher prices, or a website that falsely claims it can help lower your mortgage payments. As a competition and consumer protection agency, the FTC—an independent government agency established in 1914—has broad authority to guard against these types of unfair and deceptive practices, and go after those who engage in them.

As a Commissioner at the Federal Trade Commission—a bipartisan agency—it is my responsibility and honor to ensure that our agency is fulfilling its mission to protect consumers. And privacy and data security are among my top priorities.

I have been actively engaged in consumer privacy issues for many years. I have worked on these issues with state attorneys general throughout the United States, as a consumer protection attorney within two state AG offices, and also as head of the States' Privacy Working Group.

In my current role as an FTC Commissioner, I continue to make uses surrounding privacy and data security among my top priorities. And the privacy issues relating to the collection and use of consumer information have the full attention of the entire Commission.

As you know, the FTC has been devoting significant resources to considering whether the frameworks relied on in the past to protect consumer privacy are doing what they need to do.

In the past, we have relied heavily on the "notice and choice" model, which is based on the idea that businesses will provide consumers with understandable information about how their personal information is used. And then, based on this information, consumers will be able to make intelligent choices.

We have also relied on a framework that focuses on those practices that cause indisputable harm to consumers. For instance, lax security practices that caused a data breach that might in turn lead to identify theft—in other words, violations that might lead to quantifiable harm.

But we have discovered over time that these frameworks are lacking. Notice and choice sounds pretty simple, but in many cases it just doesn't work. It is just not reasonable to expect consumers to click through 150 screens on their mobile device just to see the privacy policy they are agreeing to. And if they are able to view it, it isn't reasonable to expect consumers to read and understand some of these privacy policies, many as simple and clear as the Code of Hammurabi.

Focusing on harm also has its limitations. First, it kicks in only after the harm has already occurred. It doesn't provide sufficient incentive to companies to develop systems that will avoid harm in the first place. Also, focusing on tangible harm is an incomplete approach because it misses very real but less quantifiable harms. Harms such as the exposure of information relating to health conditions, or information about children.

Back in 2002, the FTC pursued an action against Eli Lilly, a pharmaceutical company that disclosed hundreds of email addresses of customers who had signed up for an email reminder service in connection with an antidepressant drug.[1] While it may be difficult to attribute a dollar amount to the harm suffered by these individuals, there is no question that the exposure of this type of information is harmful.

Two more recent FTC cases demonstrate other types of real harms from the exposure of consumers' information. In one case, a company known as Teletrack developed lists of financially distressed consumers who had sought payday loans. Teletrack then sold this "sucker" list to marketers, who pitched other expensive and problematic financial products to these consumers.[2] And Google Buzz, a social networking service, was the subject of another recent FTC action because consumers' frequent email contacts were made public without their consent.[3] There were press reports about the harm resulting from this disclosure. In some cases, individuals' frequent contact with health care providers was revealed. In other cases, confidential sources of journalists were exposed.

We are already paying attention to these harms, but we need a framework that better recognizes them—and prevents them before they occur.

Advances in technology have further revealed the deficiencies of both the notice and choice and harm-based frameworks. The line between personally identifiable information and non-personally identifiable information is blurring, as technologists demonstrate the relative ease with which some de-identified information can be re-associated with specific consumers or devices.

We are not the only ones that believe we need to consider how to improve the privacy landscape. I was in Brussels just a few weeks ago where I attended several conferences with international regulators, industry participants, academics and civil society members. I also had the chance to meet with several European regulators, both from the European Commission and the European Parliament. As you may know, a new regulatory framework for privacy is now being developed in the European Union and a proposal is expected by the end of the year. As I spoke to my European colleagues, I was struck by how many of the same goals we share. And it was very clear that we both value the open lines of communication that we have worked hard to develop

[1] *In the Matter of Eli Lilly and Co.*, File No. 012 3214, Docket No. C-4047.

[2] See *U.S. v. Teletrack, Inc.*, No. 1:11-CV-2060 (N.D. Ga. filed June 24, 2011).

[3] *In the Matter of Google Inc., a corporation* FTC File No. 1023136 (2011).

over recent years. At the FTC, we see great value in the international privacy dialogue as we all work to develop solutions to better protect consumer privacy.

For our part, in order to thoughtfully consider how our approach could be improved, in 2009 the FTC launched an initiative that we refer to as our privacy "rethink." In December of 2010, based on extensive written input received from stakeholders, and in-depth discussions in a series of roundtables, the FTC staff proposed a preliminary updated framework for safeguarding consumers' personal data.[4] The proposals in the report are intended to inform policymakers, including Congress, as they develop solutions, policies, and legislation governing privacy. It is also intended to guide and motivate industry to develop best practices and self-regulatory guidelines.

First, it calls for companies to build privacy and security protections into new products. Privacy and security simply cannot be an afterthought. These issues must be considered at the outset when products and services are being developed. This concept is often referred to as "Privacy by Design."

When designing new products and services, the level of security and privacy protection should be proportional to the sensitivity of the data used. In order to build privacy and security into its products, each company should examine the information it collects about consumers—and determine whether that information is really needed. Similarly, each company should examine how long it is retaining data, and work towards retaining it only as long as it is needed.

Second, we call for simplified privacy policies that consumers can actually understand without having to go to law school at night. One way to simplify notice is to exempt "commonly accepted" practices from the first layers of notice, to help remove the clutter so that consumers can pay attention to those practices that really matter.

And third, we call for greater transparency around data collection, use and retention. Consumers should know what kind of data companies collect, and should have access to it in proportion to the sensitivity and intended use of the data.

I believe that this framework is flexible enough to allow businesses to profit and offer valuable services to consumers to enjoy the products and services on which they have come to rely. Equally important, I believe that this framework enables companies to continue to innovate.

One of the most talked-about recommendations in the report is the development of a "Do Not Track" mechanism in connection with behavioral advertising. Our vision for this mechanism would allow consumers to have some meaningful control over how their online behavioral information is used. And whether their information is collected in the first place.

---

[4] Fed. Trade Comm'n, *Protecting Consumer Privacy in an Era of Rapid Change: A Proposed Framework for Businesses and Policymakers* (2010) (preliminary FTC staff report), *available at* http://www.ftc.gov/os/2010/12/101201privacyreport.pdf.

Industry is listening and we have seen some initiative in developing these mechanisms. It is feasible. But, like anything else, it's all in the details. Successful Do Not Track mechanisms must contain certain features—we've identified five necessary elements.

- First, any Do Not Track system should be implemented universally, so that consumers do not have to repeatedly opt out of tracking on different sites.
- Second, the choice mechanism should be easy to find, easy to understand, and easy to use.
- Third, any choices offered should be persistent and should not be deleted if, for example, consumers clear their cookies or update their browsers.
- Fourth, a Do Not Track system should be comprehensive, effective, and enforceable. It should opt consumers out of all behavioral tracking through any means and not permit technical loopholes.
- Finally, an effective Do Not Track system would go beyond simply providing an opt out of receiving targeted advertisements. It should allow consumers to opt out of collection of behavioral data for all purposes other than commonly accepted practices such as product and service fulfillment.

I am encouraged by the Do Not Track capabilities released by some of the major browser vendors. Choice mechanisms for online behavioral advertising are now available in the browser products offered by Mozilla, Microsoft, and Apple. In addition, an industry coalition of media and marketing associations, the Digital Advertising Alliance, has continued to make progress on implementation of its improved disclosure and consumer choice mechanism offered through a behavioral advertising icon.

Some of you may have noticed that in the brochures my talk is entitled "Is Self-Regulation Dead?" Just for the record, PLI gave my talk this title. But it is a question worth asking. And my answer, in four words, is "Far from it, but..." All of the current efforts to build more robust self-regulatory mechanisms are truly encouraging. But many agree that more work needs to be done. These self-regulatory solutions can only work if there is full participation of the online advertising industry. We need to be sure that, no matter which mechanism is employed, the preferences of consumers are in fact honored, and that there are real consequences if they are not.

It is also important that we translate these issues and solutions into the mobile space. The mobile space operates differently from the traditional online environment, and so we need to look at its unique characteristics, including how apps operate, as we consider privacy issues in this area.

The mobile environment enables the sharing of so much information—and with so many different parties. Companies must act responsibly. A recent study by the Future of Privacy Forum found that out of the top 30 paid apps, 22 of them didn't even have a basis privacy policy.[5] I believe that companies offering products and services in the mobile space can do a much better job of informing consumers about their practices.

[5] Shaun Dakin and Shreya Vora, "FPF Finds Nearly Three-Quarters of most Downloaded Mobile Apps Lack a Privacy Policy." *Available at* http://www.futureofprivacy.org/2011/05/12/fpf-finds-nearly-three-quarters-of-most-downloaded-mobile-apps-lack-a-privacy-policy/

And turning to Do Not Track, I, for one, believe that mobile service providers and mobile browsers should provide Do Not Track mechanisms. At least one company is working towards this goal: Mozilla recently introduced a version of its browser that enables Do Not Track for web browsing on mobile devices.

I believe the need for a Do Not Track mechanism in the mobile space will only increase as more consumers live more of their lives online through their mobile devices.

Another industry segment that should address its current privacy challenges is the data broker industry. This industry faces unique transparency issues because many data brokers never engage directly with consumers and are often invisible to them.

Data brokers control details about consumers that can have a direct impact on their credit and financial well-being. I believe we may need to modernize our notions about information brokers, and perhaps even credit reporting agencies, to keep up with new methods of collecting, selling and using information about consumers for the purpose of making decisions that affect their financial lives, employment, and housing.

We've all read about businesses that "scrape" and "sniff" for information about particular consumers on the web—including on social network sites—and provide that information to insurers, lenders, and other financial firms. We've read that these financial firms then use this information to make decisions about whether—and on what terms—to provide financial products to the consumers.

When Congress created the Fair Credit Reporting Act, it created clear guidelines on how personal information can be used for credit, insurance and other services. Congress mandated that consumers have a right to know when such information is being used, and a right to access and correct it. The Federal Trade Commission, as well as the new Consumer Financial Protection Bureau, needs to make sure our current rules continue, in this technologically advanced age, to protect consumers' right to know the data that has been collected and used to make important financial decisions about them, and to correct that data when necessary.

The privacy area also raises some critically important issues relating to children. The FTC has long been committed to protecting information about children. We enforce the rule issued pursuant to the Children's Online Privacy Protection Act, known as COPPA.

In our most recent COPPA case against Playdom Inc., and one of its senior executives, the Commission obtained an agreement with the operators of 20 online virtual worlds to pay the largest civil penalty case ever in a COPPA case—$3 million—to settle charges that they violated COPPA by illegally collecting and disclosing personal information from hundreds of thousands of children under age 13 without their parents' consent. The defendants allegedly collected children's ages and email addresses during registration and then enabled the children to publicly post their full names, email addresses, instant message IDs, and location information on their personal profile pages and in online community forums.[6]

[6] See *United States of America, Plaintiff v. Playdom, Inc., a subsidiary of Disney Enterprises, Inc., and Howard Marks, Individually, Defendants*, No. SACV11-00724 (C.D. Ca filed May 12, 2011)

We are also developing creative ways to ensure that children are educated about what they are doing online. Consumer education plays a critical role in helping address harms before they occur, particularly with respect to children. The FTC has launched a number of education initiatives designed to encourage children to use technology safely and responsibly. The Commission's educational booklet, *Net Cetera: Chatting with Kids About Being Online*, provides practical tips on how parents, teachers, and other trusted adults can help children of all ages, including teens and pre-teens, reduce the risks of inappropriate conduct, contact, and content that come with living life online. *Net Cetera* focuses on the importance of communicating with children about issues ranging from cyberbullying to sexting, social networking, mobile phone use, and online privacy. The Commission has collaborated with schools, community groups, and local law enforcement to publicize *Net Cetera*, and the agency has distributed more than 7.8 million print copies of the guide since it was introduced in October 2009.

The initiatives that I have discussed with you today—enforcement, policy making and consumer education—they are a package deal. Each one is important on its own. Together they weave a strong fabric designed to protect consumers' personal information. I am committed to our work in this area, and I appreciate your interest.

Once again, thanks for inviting me to speak to you today, and thanks for listening.