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

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

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

We are also developing creative ways to ensure that children are educated about what they are