Commissioner Julie Brill
United States Federal Trade Commission

"Privacy and Responsibility:
A Call for Industry Super-Heroes"
An Address before the
Computer and Communications Industry Association
May 4, 2011

Good afternoon. Thank you for that kind introduction and for the opportunity to speak to you today. I've spent considerable time throughout my career working on and thinking about privacy, and I am thrilled to be a Commissioner at the FTC, the agency leading the federal government's efforts on privacy.

Today I'd like to take a step back and reflect on the state of privacy through the lens of the season. And although other than today, it has been lovely outside, with flowers and trees in full bloom, I don't mean springtime. I mean the just-completed tax season. Around this time of year, almost all taxpayers – both those of us who cut checks to Uncle Sam, and those of us lucky enough to get refunds – usually take a few moments to examine our personal financial ledgers, assess our assets and liabilities, and figure out the state of our financial health. Today I'd like to take a few moments to examine the nation's ledger on privacy.

Let's first look at the liability side. It is fair to say that TS Eliot was right, at least with respect to this year: "April [was] the cruelest month." We began April with the news that the online marketing company Epsilon had suffered a data breach, potentially exposing the email addresses of millions of customers of the nation's largest firms, including JP Morgan Chase, Citibank, Target and Walgreens, placing the customers of these institutions at an increased risk of email scams. Then, during the last week of April, we learned about two more major privacy snafus. Last week began with disclosures that Google and Apple have been collecting and retaining, through our smartphones, much more information about our movements throughout the day than we realized. And last week ended with news that Sony's PlayStation online network had been hacked, resulting in the exposure of the names, addresses, email addresses, user names, passwords – and in some cases credit card numbers – of about 77 million gamers worldwide.

We only have to travel back in time a few months to recount several other major privacy breaches that show up on the liability side of our ledger. Breaches that resulted in strong FTC action. At the end of March, the Federal Trade Commission announced our proposed settlement involving Google Buzz, which some have called "the most significant privacy decision by the Commission to date". This proposed settlement requires Google to put into place a number of remedial measures as a result of its collection of consumer information for one purpose – email services – and use of it for another – its launch of a social network – all in a manner that ran counter to the promises it made to consumers when the data was first collected.

Also in March, the FTC announced its settlement with an ad network, known as Chitika, for promising to provide consumers an opt out from its targeted advertising, but creating an opt

out that lasted only 10 days. And several months earlier, we announced a settlement with a company, known as EchoMetrix, that marketed a children's online security program that failed to adequately disclose that the company shared information about children with third party marketers.

Now let's take a look at the asset side of our privacy ledger. The benefits that many online companies provide to consumers and the economy are enormously significant. Targeted advertising could be said to solve the problem posed over a century ago by the great merchant and civic leader, John Wanamaker, who said: "Half the money I spend on advertising is wasted; the trouble is I don't know which half." Targeted advertising is much more valuable to companies trying to reach consumers who are more likely to be interested in their products and services, and companies are willing to pay significantly more for it. As a result, targeted advertising finances much of the free content on the web.

And targeted advertising has helped finance the explosion of social media and location-based apps that have literally transformed the way we live. Because of these innovations, we can now become friends with people whose voices we've never heard. We can reconnect with folks we knew years ago, but lost touch with. We can tweet our thoughts to a cyber café full of anyone who wants to listen. Shops can email us when it is Grandma's birthday, remind us what we got her last year – so we don't get her the same thing this year – and suggest a new present, offering to charge it on our credit card they stored.

You in this room have created for us the means to shop for groceries online – go to the movies online – share photo albums online – pay traffic tickets online – and even date online!

And as we watched the events of the Arab Spring unfold in Tunisia, Egypt, and Libya over the past few months, we have come to understand that you have given the world the means to create revolutions.

Simply put, you in this room, and the companies you represent, have tremendous power to drive innovation, create an ever richer source of information and value for consumers, and help launch significant social change. So today, as a deep admirer of all that you can do, I ask you, as you continue to create and innovate, to also remember your responsibility to manage the other side of the ledger.

I ask you to take a moment to reflect on the words of one of my heroes, Peter Parker [, Spiderman's alter ego]: "With great power comes great responsibility".

Now I do not ask you to completely play the role of superhero: I don't expect you to leap from building to building, or bring down the bad guys with only a rubber suit and mask to protect you. But I do ask you to take very seriously your responsibility to your customers, to consumers, and to society, and to remember, as you improve on the powerful online tools and mobile apps you have already provided to us, to build privacy protections into the design of your innovations.

This recognition of your power, and this call to use it responsibly, is the touchstone of the FTC's recently released preliminary privacy report, which we've called "Protecting Consumer Privacy in an Era of Rapid Change: A Proposed Framework for Business and Policymakers."

Background

Since the enactment of the Fair Credit Reporting Act in 1970, the FTC has led the federal government's efforts to protect consumer privacy. Section 5 of the FTC Act empowers us to challenge deceptive or unfair acts or practices. We also enforce a number of sector-specific statutes, including those that protect personal information about children and consumer data used in credit, employment, and other sensitive financial transactions. We implement the CAN-SPAM Act, which seeks to limit unsolicited email, and we run the national Do Not Call Registry, which Dave Barry has called the most popular government program since the Elvis stamp.

Throughout the years, the Commission has worked to preserve consumers' control over their private data, even as technology races ahead, ever developing new ways to collect, aggregate and use that data. In the 1990s, we relied primarily on a "notice and choice" model, counting on businesses to give consumers clear choices about how their data is used, and counting on consumers to read and understand privacy policies before making those choices.

The theory is sound, but it has proven unworkable. It is not reasonable to expect consumers to read and understand privacy policies – most about as long and as clear as the Code of Hammurabi – especially when all that stands between them and buying a new flat-screen TV or cute pair of boots is checking the little box that says "I consent."

So, several years ago, the Commission turned to playing defense – focusing on privacy violations that cause indisputable harm: data breaches, identity theft, invasion of children's privacy, spam, spyware, and the like. But this approach falls short as well: it only addresses infringements on privacy *after* harm has been done, giving too little incentive to companies to design systems that will not do harm in the first place. Also, by focusing only on tangible harms to consumers, this approach misses the less quantifiable – but none the less real – injuries suffered by those whose sensitive information – such as data relating to medical conditions, children, or sexual orientation – is exposed.

And both approaches have fallen short as our technology advances, presenting ever-more-sophisticated opportunities to collect data – including the ability to gather information about consumers' every move from their smartphones. And ever-more-sophisticated opportunities to manipulate data – including the ability to take information that has been stripped of personal identification and re-associate it with specific individuals.

The Report

So, with our "notice and choice" and "no harm, no foul" paradigms falling short of providing meaningful privacy protection for consumers in this advanced technological age – allowing more and more rapid data collection that is more and more invisible to consumers – the Commission proposed an updated framework for safeguarding consumers' personal data.

The report makes three principal recommendations. First, we call for companies to build privacy and security protections into new products, not just retrofit them after problems arise. When designing new products and services, the level of security and privacy protection should be proportionate to the sensitivity of the data used. And companies should limit the amount of information collected to what is needed, and retain the data only as long as needed.

Second, we call for simplified privacy policies that consumers can understand without having to retain counsel. The report suggests that one way to simplify notice is to exempt "commonly accepted" practices from the first layers of notice, to help remove the clutter. There is probably a group of practices that we can all agree are "commonly accepted" – such as sharing data with the shipping company that will deliver the product that you just ordered. By removing disclosures relating to these commonly accepted practices, consumers can focus their attention on more unexpected uses of data.

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.

When taken as a whole, I believe the framework we have proposed is flexible enough to allow businesses and consumers to continue to profit from an innovating, growing, and rich information marketplace, and also sturdy enough to provide guideposts on how to innovate and grow in a responsible manner.

Do Not Track

The Commission's most talked-about recommendation is the creation of a "Do Not Track" mechanism, to allow consumers some meaningful control over how their online behavioral information is used. I imagine this continues to be a proposal of interest to you. So I want to dispel some concerns we have heard about it.

The first is whether "Do Not Track" will become the government's next "Do Not Call" program. As many of you know, the Commission's "Do Not Call" registry lists the phone numbers of consumers who choose to opt out of certain types of telemarketing. But Do Not Track is not like Do Not Call. "Do Not Track" will not be a government run registry. There are no easily accessible persistent identifiers for computers, and creating any kind of list of IP addresses would raise its own significant set of privacy issues.

Instead, the Commission's Do Not Track proposal is preliminarily based on a technology-driven approach that will allow consumers to make persistent choices that travel with them through cyberspace, communicating their tracking preferences to every website they visit. Such an approach could allow consumers more granular choices, beyond just opting out of behavioral advertising altogether. Consumers could have meaningful control over the information they share and the sort of targeted ads they receive.

I want to commend the major browser providers, as well as the Digital Advertising Alliance, all of whom quickly rose to our challenge. They have been experimenting with how to provide these controls to consumers in a more user friendly, meaningful way. Kudos to all of you.

Some have asked me whether, in light of industry's current experimentation with Do Not Track mechanisms, it is time for the FTC to claim victory, and move on. My view is that it is too soon to judge whether industry's efforts will provide consumers with meaningful, informed notice and choice about the collection and use of their online behavior. To determine whether any Do Not Track mechanism will be successful, we have indicated we will examine it using five criteria:

- Is it easy for consumers to use;
- Does it provide consumers with persistent choices;
- Is it part of a universal program that the vast majority of industry participates in;
- Does it provide choices with respect to collection as well as use of information; and
- And is it effective and enforceable.

This brings me to a second concern we have heard about "Do Not Track" – that, given the choice, consumers en masse will opt out of behavioral advertising, drying up the ad revenue that lets us enjoy content and innovative online activities for free.

As the Commission learned during the our discussions and research prior to issuing our report, when given an informed and more granular choice, most consumers, including myself, want to receive tailored ads – and will choose to share information for that purpose.

This entire discussion about the dilemma advertisers believe they are in reminds me of a quintessential movie of another season, "Miracle on 34th Street." For those of you too young to have seen it, the movie is about a Macy's Santa Claus who listens to children's Christmas wishes, then sends their parents to other stores if Macy's doesn't have exactly what their children want. Of course, the personal attention is a huge hit with shoppers. Mr. Macy himself says: "No high pressuring and forcing a customer to take something he doesn't really want. We'll be known as the helpful store…the store that places public service ahead of profits. *And, consequently, we'll make more profits than ever before."*

Mr. Macy would not have had a problem with "Do Not Track." He would have recognized that providing consumers with meaningful choices increases his credibility and can grow, rather than shrink, his market share. He would have been eager to compete with respect to privacy.

"Do Not Track" provides an opportunity to businesses and ad networks to convince consumers they will handle personal data with care and put the information to good use in serving them, so that consumers will not want to opt out. I have no doubt the marketing departments of companies selling on the Internet, and their ad networks, are up to the task of creatively informing consumers about the benefits of collecting and using their information to provide more personalized advertising. The alternatives – not informing consumers about what

is happening, or obscuring the truth and creating obstacles to making choices – is simply not palatable.

Data Collection and Information Brokers

There is one more aspect of the report I want to highlight for you. The goals of greater transparency, and providing reasonable access to information collected that is proportional to both the sensitivity of the data and how it is to be used, are particularly important with respect to information brokers. These are entities that never engage consumers directly and are often invisible to them. Yet 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 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 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 it is being used, and a right to access and correct it. The Federal Trade Commission and the new Consumer Financial Protection Bureau need 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.

Conclusion

A couple of years ago, Rupert Murdoch told the Commission that "from the beginning, newspapers have prospered for one reason: the trust that comes from representing their readers' interests and giving them the news that's important to them." Mr. Murdoch called on the media to "innovate like never before", delivering "the news … consumers want … in the ways that best fit their lifestyles."

I expect all of you want to follow Mr. Murdoch's call to "innovate like never before" and yet to earn consumers' trust. So go on, use your power and talents to build a web that is vast, robust, and beneficial – and as you build that web, earn consumers' trust by building in privacy and security protections.

Go on, be a little like Spider-Man.

Thank you.