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

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

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 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.