Remarks of
Federal Trade Commissioner Julie Brill
at the National Cyber Security Alliance
Data Privacy Day
January 26, 2012

Good morning, and thank you to the organizers of today's event for inviting me. In particular, let me thank the National Cyber Security Alliance—an organization committed to ensuring that the online world is a trusted destination.

At the Federal Trade Commission, our mission is to create and promote trusted destinations. We protect the nation's consumers as they navigate the marketplace, and protect competition as it shapes the economy. Safeguarding consumer privacy is essential to our mission.

Consumers should not have to give up control over their most sensitive data as the toll to enter the information superhighway. The disclosure of personal information such as health, finances, and location can, in some instances, have disturbing consequences.

And exacting such a toll is just bad business: no market can function if consumers feel unsafe participating in it—if they believe they have no decisions about how their information is used, or their decisions about what information to share and what to keep private are not respected.

This, of course, is the great challenge of the growing, exciting, and innovative cyber-market, much of it based on the exchange of information, much of that information sensitive and private. Companies' efforts to keep online data secure are an important part of the equation in determining whether they meet that challenge.

We don't have to look very far to find examples that make this point—like the 24 million Zappos customers, myself included, who are busy changing passwords and will think twice next time they click to buy that perfect pair of black boots. As Zappos CEO Tony Hsieh wrote in an

email, "We've spent over 12 years building our reputation, brand, and trust with our customers. It's painful to see us take so many steps back due to a single incident."

So, on behalf of consumers, and businesses that work to earn their trust, I am delighted to participate in Data Privacy Day—though I think most of us would say what I used to say to my boys when they asked why there is a Mother's Day and a Father's Day but no Children's Day: "Every day is Children's Day." And so I say to you today, every day is Data Privacy Day—or at least it should be.

Or really, every day is "Data Privacy and Data Security Day" because as we all know, the two go hand in hand. But I admit that "Data Privacy Day" is catchier, and so I'm fine with the shorter name.

Really, it is not the name of the Day that is important, but rather, what the Day represents, and even more importantly, what actions are taken, guided by the principles we espouse on this commemorative day.

I can't help but think back to just over a week ago when we celebrated Martin Luther King, Jr.'s birthday. As much as anyone in our history, Dr. King lived to make real the principles embedded in the founding of our Nation—justice and fairness. He expressed the promise of these principles in soaring rhetoric that stands with the Declaration of Independence as an expression of what America is—or should be.

The day we set aside to honor Dr. King is not just a day to remember the man, but it is a day that we undertake acts of service—working at a local food bank, volunteering at a senior center, or reading to our kids about Dr. King and his legacy—concrete steps toward the promised land he saw from the mountaintop. Believing in the principle is important. But taking those principles and putting them into practice is what really matters.

At the FTC, we have undertaken considerable effort to work towards establishing principles that are critical in protecting consumers' privacy and keeping their information secure.

We have both provided guidance to industry through our reports and policy work, and incentives to industry through our enforcement actions, to take these principles and put them into practice.

In December 2010, the FTC issued a preliminary report on privacy that laid out basic guidance towards a framework that protects consumer information, and enables businesses to continue to thrive and innovate.[1]

The first principle is "Privacy by Design." To translate this principle into practice, industry should build privacy and security protections into new products. Examine the information you collect about consumers and determine whether you really need to collect it. Determine how long you are retaining data and figure out how long you really need to keep it.

The second principle is "Simpler Choice." Our recommendation to implement Do Not Track mechanisms is but one example of how this principle would be put into practice in the behavioral advertising area. Industry has been working on Do Not Track—we're now seeing two types of these mechanisms. One is a solution at the browser level, and the other is an icon-based opt-out program.

The success of Do Not Track hinges on a critical mass of industry players – including advertisers and ad networks – participating and fully honoring the choices that consumers make. And the success of Do Not Track also hinges on how these two mechanisms will work together.

Developers of each mechanism should move quickly to make sure that the user's choice will be honored, no matter which mechanism is used to express that choice. This will ensure that the important "simplified choice" principle is translated into practice for all consumers that have expressed a choice.

The third principle is "Greater Transparency"—companies should provide consumers with more information about what is being done with their personal information. One way of

[1] *See* A Preliminary FTC Staff Report on Protecting Consumer Privacy in an Era of Rapid Change: A Proposed Framework for Businesses and Policymakers (Dec. 1, 2010), *available at* http://www.ftc.gov/os/2010/12/101201privacyreport.pdf.

putting this principle into practice is providing consumers with access to the information about them that a company possesses. Access is critical, particularly when we're talking about entities that consumers can't identify or don't even know exist—like data brokers. These entities control details about consumers that can have a direct impact on their credit, employment status, and financial well-being. We are also seeing entities that combine data from multiple sources, including off line and social networks. We have seen researchers and some companies pull these data points together to make predictions about consumers' future behavior. I have long been concerned about data that are used in place of traditional credit reports, to make predictions that become part of the basis for making determinations regarding a consumers' credit, their ability to secure housing, gainful employment, or various types of insurance.

We've seen press reports about how life insurers use consumer consumption patterns to predict life expectancy – and hence to set rates and coverage the insurers offer for their policies.[2] Analysts are undoubtedly working right now to identify certain Facebook or Twitter habits or activities as predictive of behaviors relevant to whether a person is a "good" or "trustworthy" employee, or is likely to pay back a loan. Might there not be a day very soon, when these analysts offer to sell information scraped from social networks to current and potential employers to be used to determine whether you'll get a job or promotion? Or to the bank where you've applied for a loan, to help it determine whether to give you the loan, and on what terms?

I am calling on data brokers to take the transparency principle and put it into practice. Develop a user friendly one-stop shop where consumers can gain access to information that data brokers have amassed about them and, in appropriate circumstances, can correct that information. Data brokers need to get cracking now to putsomething like this into place.

The Commission's call to translate principles into practice is heard loud and clear through our enforcement work in both the data security and privacy areas.

[2] Leslie Scism, Mark Maremont, *Insurers Test Data Profiles to Identify Risky Clients*, The Wall Street Journal November 19, 2010.

Our data security actions involve companies in a variety of sectors—online retailers, payroll processors, pharmacies, and more. Despite this variety, our message is consistent—companies that fail to implement reasonable security safeguards to protect consumer information will come under our scrutiny.

The consent orders in these cases generally require companies to implement a comprehensive data security program and obtain independent audits for 20 years. The data security programs require these companies to put data security principles into practice. And the third-party assessors examine the program's implementation to determine how the program is actually working on the ground.

Anyone can have a program—it's putting the program into practice that is the important part. I can't help but recall that Seinfeld episode where Jerry is frustrated at the rental car counter when the company's employees admit they have his reservation, but that they've run out of cars. Jerry makes the point that anyone can take a reservation—it's honoring the reservation that is the important part. It is the same thing when it comes to the data security programs we require—it's not enough to have the program in place; the program needs to be working.

Reasonably safeguarding consumer information is critical to a trusted online marketplace. And nothing demonstrates the importance of this issue more than its unanimous bipartisan support. At the Commission, all of my colleagues are on board in support of legislation that would require companies to implement reasonable data security policies and procedures and, in appropriate circumstances, provide notification to consumers when there is a security breach.

Our enforcement actions in the privacy area are also a call to industry to put important privacy principles into practice. Facebook and Google learned this the hard way.

The Commission's complaint against Facebook alleges a number of deceptive and unfair practices in violation of Section 5 of the FTC Act.[3] These include the 2009 changes made by Facebook so that information users had designated private became public. We also addressed

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

Facebook's inaccurate and misleading disclosures relating to how much information about users apps operating on the site can access.

We were also concerned that the company misrepresented its compliance with the U.S.-EU Safe Harbor. And we called Facebook out for promises it made but did not keep: It told users it wouldn't share information with advertisers, and then it did; and it agreed to take down photos and videos of users who had deleted their accounts, and then it did not.

The proposed FTC settlement with Facebook prohibits the company from misrepresenting the privacy and security settings it provides to consumers. Facebook must also obtain users' "affirmative express consent" before sharing their information in a way that exceeds their privacy settings, and it must block access to users' information after they delete their accounts. Borrowing a page from our data security enforcement playbook, we also require Facebook to implement a comprehensive privacy program that an independent auditor will monitor for 20 years.

In October of last year, the FTC finalized a similar enforcement action against Google, arising from Google's first social media product, Google Buzz.[4] We believed that Google did not give Gmail users good ways to stay out of or leave Buzz, in violation of Google's privacy policies. We also believed that users who joined, or found themselves trapped in, the Buzz network had a hard time locating or understanding controls that would allow them to limit the personal information they shared. And we charged that Google did not adequately disclose to users that the identity of individuals who users most frequently emailed could be made public by default. The Google Buzz complaint also included an allegation relating to the failure to comply with the requirements of the U.S.-EU Safe Harbor.

Like Facebook, Google settled our complaint. And like Facebook, Google is also required to implement a comprehensive privacy program and to obtain periodic assessments that will examine how well the privacy program is put into practice.

[4] *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.*

I started out my remarks today with a reference to Mother's Day. And so I can't help but think about one of my mother's favorite sayings: "Julie, there's always room for improvement."

We can always continue to strive to improve and better implement the principles that we have developed to protect the privacy of consumers' information and to keep the information secure.

And as an enforcement body, we also know that, just as my mother said, our work is never done. One important area where we continue to make inroads is developing a more robust framework to cooperate with our international counterparts. Data Privacy Day is celebrated around the world. Our foreign colleagues are also coming together on this day to shine a spotlight on the importance of privacy and data security.

One of my priorities since joining the Commission is to further strengthen our work internationally. The FTC is a major contributor in the international privacy community, and with a number of our colleagues, we continue to develop mechanisms to enable us to cooperate on enforcement matters, including the sharing of information. Through the OECD, APEC, the Global Privacy Enforcement Network and the International Conference of Data Protection and Privacy Commissioners, we are working hard to build on our strong foundation of international enforcement cooperation.

So thanks very much for inviting me here and giving me the opportunity to spend some time with you this morning. And Happy Data Privacy Day!