Opening Statement of FTC Commissioner Julie Brill
U.S. House of Representatives Energy and Commerce Committee
Privacy Working Group
Washington, DC
April 8, 2014

Good afternoon Representative Blackburn, Representative Welch, and Members of the Working Group. It is a pleasure to be here to discuss consumer data privacy.

My name is Julie Brill, and I have served as a Commissioner of the FTC since 2010.

Protecting consumer privacy is one of the FTC's top priorities. Before I go into some detail about how we protect consumer privacy, I'd like to spend a moment explaining why privacy is an important area of our focus.

The amount of data that companies collect, retain, use, combine, and disclose has grown exponentially over the past few decades. Data about each of us and our activities – our personal information – is an increasingly important part of the U.S. economy. The flow of personal information goes hand-in-hand with many of the innovations that allow us to connect with friends, find our way around cities that we've never visited before, and collaborate with colleagues around the world.

Privacy and data security protections are essential to maintaining consumers' confidence in this expanding and innovative digital economy. Privacy also has become an inescapable subject of dialogue with our international trade partners.

As technology has evolved, companies have become much more sophisticated about collecting, analyzing, and using data about consumers. Big data – the massive and growing amount of personal information available to companies – fuels this analysis. These developments can give rise to enormous benefits for consumers, companies and society at large.[1] They can also give rise to privacy harms that can be concrete, or can be intangible and harder to quantify but nonetheless real. Big data analytics allows companies to sort and segment consumers according to sensitive characteristics like health condition, financial status, religion, and sexual orientation, sometimes based on inferences from innocuous data.[2] Security breaches involving such sensitive information can be devastating to consumers. In addition, consumers believe they are exposed and vulnerable in an environment in which they are tracked and their

[1] *See, e.g*, Timothy Hunter, Traffic Jams, Cell Phones, and Big Data, UC Berkeley AmpLab Blog, Jan. 18, 2012, *available at* https://amplab.cs.berkeley.edu/2012/01/18/traffic-jams-cell-phones-and-big-data/; Brian Proffitt, *Big Data Analytics May Detect Infections Before Clinicians*, ITWORLD, Apr. 12, 2012, *available at* http://www.itworld.com/big-datahadoop/267396/big-data-analytics-may-detect-infection-clinicians; Lisa Wirthman, *How First Responders Are Using Big Data To Save Lives*, FORBES EMCVOICE, Jan. 10, 2014, *available at* http://www.forbes.com/sites/emc/2014/01/10/how-first-responders-are-using-big-data-to-save-lives/#.

[2] *See* Joseph Walker, *Data Mining to Recruit Sick People*, WALL ST. J. (Dec. 17, 2013), *available at* http://online.wsj.com/news/articles/SB10001424052702303722104579240140554518458; Charles Duhigg, *How Companies Learn Your Secrets*, N.Y. TIMES MAGAZINE (Feb. 16, 2012), *available at* http://www.nytimes.com/2012/02/19/magazine/shopping-habits.html.

information is collected and used for purposes outside the context of their online transactions. In some cases, consumers avoid companies that they do not believe they can trust with their personal information.[3] But in many cases, consumers do not really know what these non-consumer facing companies do with their data, what choices consumers may have about this data use, and what protections are in place for consumers' privacy interests.

In our policy work, the FTC has developed best practices and recommendations regarding how companies can be transparent about their practices and help consumers make meaningful choices about the use of their personal information. Working toward these goals helps to ensure that consumers have confidence in the dynamic and ever-changing marketplace for personal information.[4] In addition, we hope to issue our 6(b) report about the collection and use practices of nine data brokers – companies that collect online and offline information and create rich profiles about consumers – to help provide a deeper understanding about the practices of some of these companies.

In our enforcement work, we pay particularly close attention to children's online privacy, as mandated by Congress in the Children's Online Privacy Protection Act.[5] We also enforce the Fair Credit Reporting Act.[6] Enacted in 1970, the FCRA has proven to be a durable source of consumer protections where traditional credit reports are concerned. Moreover, FCRA protections apply to uses of information, rather than specific technologies. As a result, the FCRA is a valuable source of consumer protections as consumer reporting activities draw information from more diverse sources[7] and become available through mobile devices.[8]

The bulk of our enforcement cases – brought over the past decade, under both Republican and Democratic leadership – have challenged deceptive and unfair data security and privacy practices under Section 5 of the FTC Act. In that time period, we have brought more than 50 cases against companies that, we believe, failed to reasonably secure consumers' information, and more than 40 cases relating to the privacy of consumer data. Some of these cases involve

---

[3] *See* Tim Peterson, *Customers Becoming Less Trusting of Google, Warier of Facebook, Twitter*, AD AGE DIGITAL (Jan. 9, 2014), *available at* http://adage.com/article/consumer-electronics-show/consumers-trusting-google-warier-facebook-twitter/290992/ (reporting on consumers' "eroding" trust in Facebook, Twitter, and Google).

[4] Fed. Trade Comm'n, *Mobile Privacy Disclosures: Building Trust Through Transparency* (Feb. 1, 2013), *available at* http://www.ftc.gov/os/2013/02/130201mobileprivacyreport.pdf (staff report); Fed. Trade Comm'n, *Protecting Consumer Privacy in an Era of Rapid Change* (2012), *available at* http://www.ftc.gov/os/2012/03/120326privacyreport.pdf.

[5] Children's Online Privacy Protection Act, 15 U.S.C. § 6801 et seq.

[6] Fair Credit Reporting Act, 15 U.S.C. § 1681 et seq. (2006).

[7] United States v. Spokeo, Case CV-12-05001 (C.D. Cal. June 7, 2012) (consent decree and order for civil penalties).

[8] In the Matter of Filiquarian Publishing, LLC et al., Case C-4401 (Apr. 13, 2013) (consent order); Fed. Trade Comm'n, FTC Warns Marketers That Mobile Apps May Violate Fair Credit Reporting Act (Feb. 7, 2012), http://www.ftc.gov/news-events/press-releases/2012/02/ftc-warns-marketers-mobile-apps-may-violate-fair-credit-reporting.

household names, such as Google and Facebook.[9] But we have also brought myriad cases against less well-known companies, alleging that they spammed consumers,[10] violated commitments in their privacy policies,[11] installed spyware on consumers' computers,[12] or otherwise crossed the lines of deception or unfairness in their data collection and use practices.

With respect to data security, the FTC uses its Section 5 unfairness and deception authority to ensure that companies provide reasonable security for personal information. We are all too familiar with the potential for harm from financial information falling into the wrong hands. The FTC has alleged in numerous actions that companies violated Section 5 by failing to reasonably protect consumers' financial information.[13] We received a vivid reminder about the importance of data security during the height of the holiday shopping season, when Target acknowledged that 40 million consumers' credit card and debit card information, as well as contact information about some 70 million consumers, had been stolen.[14] The movement toward innovative other forms of payment from mobile devices may create new challenges to securing financial information, and the FTC is watching these developments closely.[15]

From my perspective, there is no data privacy without data security. Inadequate data security can expose information that consumers never meant to put on public display.[16] Security

---

[9] In the Matter of Google, Inc., FTC File No. 102 3136 (Oct. 13, 2011), *available at* http://ftc.gov/os/caselist/1023136/111024googlebuzzdo.pdf (decision and order); In the Matter of Facebook, Inc., FTC File No. 092 3184 (July 27, 2012), *available at* http://www.ftc.gov/os/caselist/0923184/120810facebookdo.pdf (decision and order).

[10] *See, e.g.*, United States v. ValueClick, Inc., Case No. CV08-01711 (C.D. Cal., Mar. 17, 2008), *available at* http://www.ftc.gov/os/caselist/0723111/080317judgment.pdf (stipulated final judgment).

[11] *See* In the Matter of Chitika, Inc., FTC Docket No. C-4324 (June 7, 2011), *available at* http://ftc.gov/os/caselist/1023087/110617chitikado.pdf (decision and order).

[12] *See, e.g.*, FTC v. CyberSpy Software, LLC, Case No. 6:08-cv-01872-GAP-GJK (M.D. Fla., Apr. 22, 2010), *available at* http://www.ftc.gov/os/caselist/0823160/100602cyberspystip.pdf.

[13] *See* In the Matter of the TJX Cos., Inc., No. C-4227 (F.T.C. July 29, 2008) (consent order); CardSystems Solutions, Inc., No. C-4168, 2006 WL 2709787 (F.T.C. Sept. 5, 2006) (consent order); DSW, Inc., No. C-4157, 2006 WL 752215 (F.T.C. Mar. 7, 2006) (consent order); United States v. ChoicePoint Inc., Case No. 1:06-cv-00198-GET (N.D. Ga. Jan. 30, 2006) (stipulated final order); BJ's Wholesale Club, Inc., 140 F.T.C. 465 (2005) (consent order).

[14] MSN Money, Target: Data Breach Caught up to 70M Customers (Jan. 10, 2014), http://money.msn.com/business-news/article.aspx?feed=AP&date=20140110&id=17248581&ocid=ansmony11.

[15] *See generally* Fed. Trade Comm'n, *Paper, Plastic . . ., or Mobile? An FTC Workshop on Mobile Payments* (Mar. 8, 2013), available at http://www.ftc.gov/news-events/press-releases/2013/03/ftc-staff-report-examines-growing-use-mobile-payments.

[16] *See* In the Matter of Twitter, Inc., Case C-4316 (F.T.C. Mar. 2, 2011) (decision and order) (alleging that a failure to provide reasonable security measures led to unauthorized disclosure of nonpublic communications and personal information).

lapses can leave our children exposed in alarming ways.[17] And inadequate security in one link can weaken the security in the whole chain of software and hardware in our devices and apps.[18]

The technologies that consumers use to shop, chat, and work online are undoubtedly complex and rapidly changing. However, we also know that it is more effective for companies to protect consumer information through reasonable policies and procedures that span the entire product lifecycle, rather than waiting until after a breach. As more and more devices become networked, with a greater volume and variety of personal information flows, the costs of security failures only stand to increase.

Yesterday, a federal district court that is hearing the Commission's case against Wyndham affirmed the Commission's use of its unfairness authority to take action against companies that fail to provide reasonable and appropriate safeguards for consumers' data.[19] I applaud this decision and expect that the Commission will continue to use its unfairness authority in data security cases. Yet I also believe that federal data security legislation is needed and that it would be very useful for this Working Group to consider appropriate legislative proposals.

Let me turn very briefly to some emerging privacy issues that the FTC is currently addressing. In November, we held a workshop on the Internet of Things, to explore data security and privacy issues related to connected devices.[20] Both Commissioner Ohlhausen and I attended the Consumer Electronic Show in January, where we saw first-hand the incredible growth in the connected devices sector, including smart cars, smart clothing and wearable accessories, smart appliances, and more. I expect that in the coming months we will issue a report on some of the privacy and security issues that arise with respect to connected devices. Also in the past two months, the FTC held seminars on two cutting-edge issues:

- mobile device tracking in retail and other business ; and
- alternative scoring products that use predictive scoring to determine consumers' access to products and offers.

And on May 9, we will hold a third seminar on consumer-generated health information provided to entities that are not covered by HIPAA, including health information from wearable devices.[21]

---

[17] *See* In the Matter of TRENDNet, Inc., FTC File No. 122 3090 (Sept. 2013) (consent order).

[18] *See, e.g.*, In the Matter of HTC America Inc., Case C-4406 (F.T.C. June 25, 2013) (decision and order).

[19] Fed. Trade Comm'n v. Wyndham Worldwide Corp. Civil Action No. 13-1887 (ES) (Apr. 7, 2014), at 10-15, (denying Wyndham's motion to dismiss).

[20] Fed. Trade Comm'n, Internet of Things: Privacy and Security in an Interconnected World (Nov. 19, 2013), http://www.ftc.gov/bcp/workshops/internet-of-things/.

[21] Fed. Trade Comm'n, FTC to Host Spring Seminars on Emerging Consumer Privacy Issues (Dec. 2, 2013), http://www.ftc.gov/news-events/press-releases/2013/12/ftc-host-spring-seminars-emerging-consumer-privacy-issues.

As our past work and our planned initiatives for the coming year show, the FTC has a strong record of identifying emerging privacy and data security issues, collecting input from all stakeholders representing a variety of perspectives, and proceeding carefully to develop recommendations for policymakers and best practices for industry and consumers.

I look forward to discussing these issues with this working group today, and with you and your colleagues, industry, civil society, academics and consumer groups in the coming months.