Protecting Consumer Privacy in a Big Data Age
Federal Trade Commission Chairwoman Edith Ramirez
The Media Institute
Washington, DC
May 8, 2014

Thank you for the opportunity to speak today about the Federal Trade Commission, big data, and consumer privacy. As those of you who write the news – and those who merely read it – know, big data is, well, big.

Big data offers the promise of breakthroughs in areas as important as health care, education, the environment, and public safety, to name just a few. Some say it will revolutionize how we live, work, and think.[1] But, as is by now well-recognized, it will also have significant ramifications for consumer privacy. That's where the FTC enters the picture. As the country's primary agency charged with protecting privacy in the commercial sphere, the FTC actively uses its civil enforcement authority and research and policy function to help ensure that consumers can enjoy the benefits of technological innovation confident that their information will be used responsibly.

This afternoon I'd like to discuss some of the FTC's most recent efforts to advance this goal. I will touch on three areas: the mobile ecosystem, data security, and predictive analytics, and end with some thoughts about areas for further work.

I. What is Big Data?

At the outset, let me address what I mean by "big data." Precise technological definitions aside, "big data" has come to stand for the ability to aggregate and analyze massive data sets, which can be parsed to identify previously undetectable patterns. It's no surprise that data sets

[1] *See* VIKTOR MAYER-SCHÖNBERGER & KENNETH CUKIER, BIG DATA: THE REVOLUTION THAT WILL TRANSFORM HOW WE LIVE, WORK, AND THINK (2013).

are expanding exponentially. Each of us now produces so much information that a full 90 percent of the data in the world was created in just the last two years.[2] This upsurge in data will greatly accelerate as we embark on the "Internet of Things," when smart TVs, cars, appliances, medical devices, and even clothing will communicate with each other, and with us, each generating vast new quantities of data.

II. Protecting Consumers Across the Mobile Ecosystem

Today, smartphones are generating much of this data, with consumers reaching for them, on average, an astonishing 150 times a day.[3] The FTC is seeking to ensure that each time consumers use a smartphone or tablet, they are protected throughout the mobile ecosystem.

Last year, for instance, we sued HTC America for negligently injecting security vulnerabilities in its devices that put sensitive consumer information at risk.[4] We have also called on mobile platforms and operating systems to use their critical role in the mobile environment to ensure that consumers have a say over who has access to their data.[5] And we have brought a series of cases against individual apps that have engaged in deceptive privacy practices. These include cases against a popular flashlight app that failed to disclose to iPhone

---

[2] *Big Data, for better or worse: 90% of world's data generated over last two years*, SCIENCE DAILY (May 22, 2013), *available at* http://www.sciencedaily.com/releases/2013/05/130522085217.htm.

[3] Liz Gannes, *The Best of Mary Meeker's 2013 Internet Trends Slides*, ALLTHINGSD (May 29, 2013), *available at* http://allthingsd.com/20130529/the-best-of-mary-meekers-2013-internet-trends-slides.

[4] *See HTC Am., Inc.*, No. C-4406 (F.T.C. June 25, 2013), *available at* http://www.ftc.gov/sites/default/files/documents/cases/2013/07/130702htcdo.pdf.

[5] FED.TRADE COMM'N STAFF, MOBILE PRIVACY DISCLOSURES: BUILDING TRUST THROUGH TRANSPARENCY 15-21 (Feb. 2013), *available at* http://www.ftc.gov/sites/default/files/documents/reports/mobile-privacy-disclosures-building-trust-through-transparency-federal-trade-commission-staff-report/130201mobileprivacyreport.pdf.

users that it was sharing their location data with advertising networks,[6] and a social networking app called Path that took the full contents of users' address book without their permission.[7]

Today, we are announcing our latest case in the mobile arena – a settlement with Snapchat.[8] Launched in 2011, Snapchat has quickly become one of the most frequently downloaded apps for sharing photos and videos. Many of Snapchat's users were undoubtedly attracted by Snapchat's promise that photos and videos shared through the service – what it calls "snaps" – would self-destruct seconds after opening. Snapchat also promised its users that it would notify them if a recipient of a snap took a screenshot of the image.

The FTC has alleged that, in actuality, this private messaging service was less than discreet. There are several simple ways that recipients can save snaps indefinitely, such as through widely-available apps. In addition, there is an easy way for many recipients to prevent notice of a screenshot from being sent.

As a private messaging app, Snapchat should have also ensured that messages went to the right people. Yet a number of consumers complained that they had sent snaps to someone under the false impression that they were communicating with a friend. As alleged in our complaint,

---

[6] *See Goldenshores Technologies, LLC*, No. C-4446 (F.T.C. Mar. 31, 2014), *available at* http://www.ftc.gov/system/files/documents/cases/140409goldenshoresdo.pdf.

[7] *See United States v. Path, Inc.*, No. CV-00448-RS (N.D. Cal. Filed Feb. 8, 2013) (consent order), *available at* http://www.ftc.gov/sites/default/files/documents/cases/2013/02/130201pathincdo.pdf; *see also, Credit Karma, Inc.*, No. 132-3091 (F.T.C. Mar. 28, 2014) (proposed consent agreement), *available at* http://www.ftc.gov/system/files/documents/cases/140328creditkarmaorder.pdf; *Fandango, LLC*, No. 132-3089 (F.T.C. Mar. 28, 2014) (proposed consent order), *available at* http://www.ftc.gov/enforcement/cases-proceedings/132-3089/fandango-llc. For a collection of FTC press releases on the agency's mobile cases, see http://www.ftc.gov/news-events/media-resources/mobile-technology.

[8] *Snapchat, Inc.*, FTC File No. 132 3078 (May 8, 2014) (proposed complaint and consent order).

The FTC announces its enforcement action against Snapchat in conjunction with coordinated international efforts to protect mobile privacy. This week the Asia-Pacific Privacy Authorities forum, in which the FTC participates, is focusing on mobile privacy for the forum's Privacy Awareness Week. *See* www.privacyawarenessweek.org. As a related initiative, more than two dozen privacy authorities are taking part in a law enforcement sweep organized by the Global Privacy Enforcement Network (GPEN) to review mobile app privacy practices. GPEN brings together privacy enforcement authorities to promote and support global cooperation in cross-border enforcement of laws protecting privacy. For information about GPEN, see www.privacyenforcement.net.

this occurred because Snapchat failed to verify users' phone numbers during registration. As a result, users could, and sometimes did, register with Snapchat using another person's phone number, resulting in complete strangers receiving snaps intended for someone else. In addition, in December 2013, Snapchat's security failures allowed attackers to compile a database of 4.6 million Snapchat usernames and phone numbers, as our complaint alleges.

Having marketed itself to consumers as a private messaging service that allowed users to send messages that would "disappear forever," Snapchat was obligated to live up to those claims. While the FTC encourages the development of privacy-protective products and services, we will be vigilant to ensure that companies promising privacy as a feature are keeping their promises.

To resolve these and a number of other allegations of privacy and security violations, Snapchat will be required to implement a comprehensive privacy program and submit to outside audits. The FTC's consent order also prohibits Snapchat from misrepresenting the extent to which it maintains the privacy, security, or confidentiality of users' information.

III. Promoting Sound Data Security

The Snapchat case vividly illustrates that there is no data privacy without data security. And recent, well-publicized breaches remind us that consumer data is at risk from criminals who seek to exploit network vulnerabilities. This occurs against the backdrop of identity theft, which has been the FTC's top complaint for the last 14 years. As the sheer volume of consumer data grows, this issue will only take on added importance. And the advent of the Internet of Things means that data security will also have ramifications for the safety of our cars, medical devices, and homes.

Despite the threats posed by data breaches, I am concerned that many companies continue to underinvest in data security and make fundamental mistakes when it comes to

protecting sensitive consumer information. For example, the FTC's enforcement work in this area has shown that some companies fail to take even the most basic security precautions, such as failing to update antivirus software or to require network administrators to use strong passwords. Others have observed this as well. For example, a Verizon report on data breaches found that 78 percent of initial intrusions were of "low" or "very low" difficulty in 2012.[9]

To help reverse this trend, the FTC has sought and obtained more than 50 consent orders against companies that we charged with failing to take reasonable measures to protect consumer data. While a number of these cases involved breaches of payment card data, many others involved Social Security numbers, account passwords, health data, and information about children. And they cover a spectrum of industries and platforms – from retailers, to financial firms, to social networks, to mobile.

The FTC will continue its active data security program. Our goal is to encourage companies to make safeguarding sensitive consumer data a priority. Where needed, we will litigate these claims, as demonstrated by our ongoing court case against the Wyndham hotel chain, which suffered three breaches in an 18-month period due to what the FTC has alleged were unreasonable security practices.[10] Last month, in a much-awaited decision, the district court in the *Wyndham* case affirmed the FTC's authority to bring such cases to protect consumers under the unfairness authority of Section 5 of the FTC Act.[11]

While I am pleased with the recent *Wyndham* decision, the time has come for Congress to take further action in this area. Our bipartisan Commission has called on Congress to enact a

---

[9] 2013 VERIZON DATA BREACH INVESTIGATIONS REPORT 6, *available at* http://www.verizonenterprise.com/DBIR/2013/.

[10] *See FTC v. Wyndham Worldwide Corp.*, No. CV-01887-ES-JAD (D. Ariz. Filed Aug. 9, 2012), *available at* http://www.ftc.gov/sites/default/files/documents/cases/2012/08/120809wyndhamcmpt.pdf.

[11] *FTC v. Wyndham Worldwide Corp.*, No. CV-01887-ES-JAD (D.N.J. Filed April 7, 2014) (denying mot. to dismiss).

strong national breach notice and data security law. Among other things, we believe it is essential that such a law both require companies to notify consumers in the event of a breach and give the FTC the power to seek fines in appropriate cases in which companies have failed to implement reasonable data security safeguards – authority that we generally lack today. Allowing the FTC to seek civil penalties for violations is an important deterrent against lax security practices.

IV. The Privacy Ramifications of Predictive Analytics

Let me turn to some of the privacy ramifications of the wider use of big data analytic tools and the near ubiquitous collection of personal information that we can expect to be the norm in a big data world, especially with the rise of the Internet of Things. This is an issue that the FTC has been exploring in a variety of workshops, studies, and reports. And a week ago the White House joined the conversation in a significant report on the opportunities and privacy challenges from big data, which makes a valuable contribution to the policy debate.[12]

A. Unlimited Data Collection and Simplified Consumer Choice

As a threshold matter, some industry members argue that to fully realize the benefits of big data, businesses should not face limits on the collection and retention of data.[13] We are told that the very value of big data lies in unanticipated uses and, as a result, companies should not be restrained with regard to the amount of data that they can collect or how long they may keep it.

I take a different view. At least when it comes to consumer data, we need sensible limits on the collection and retention of personal information about individuals. In particular, as the

[12] *See* EXECUTIVE OFFICE OF THE PRESIDENT, BIG DATA: SEIZING OPPORTUNITIES, PRESERVING VALUES (May 2014) ("White House Big Data Report"), *available at* http://www.whitehouse.gov/sites/default/files/docs/big_data_privacy_report_may_1_2014.pdf

[13] *See, e.g.*, Craig Mundie, *Privacy Pragmatism: Focus on Data Use Not Data Collection*, FOREIGN AFFAIRS (Mar./Apr. 2014), *available at* http://www.foreignaffairs.com/articles/140741/craig-mundie/privacy-pragmatism; Centre for Information Policy Leadership, *Big Data and Analytics: Seeking Foundations for Effective Privacy Guidance* (Feb. 2013), *available at* http://www.hunton.com/centre_big_data_and_analytics/.

Commission advocated in its Privacy Report issued in March of 2012, companies should only collect and keep information needed for a specific business purpose.[14] And context is critical. Before data is collected or used in a way that is surprising – that is, inconsistent with the context of the consumer's interaction or relationship with a business – consumers should be given a say, in a simple, straightforward manner outside of a privacy policy.

Many businesses argue that these principles are unworkable in a big data world. The argument goes that we should focus our energy on identifying what *uses* of consumer data are appropriate, and not worry about limits on the collection or retention of data or whether consumers have a say in the process.

There is no question that we need more dialogue on acceptable and impermissible uses of consumer data. I welcome greater attention to the question of the uses that pose the greatest risk of injury to consumers and those that are harmless or beneficial. However, I remain of the view that to protect consumers, reasonable limits on data usage are necessary but not sufficient.

Let's go back to basics. Big data doesn't start as big data. Instead, it is assembled bit by bit from "little" data – each tap of a smartphone, click of a mouse, or movement detected by a sensor – and becomes "big" only when compiled into vast databases. In light of the predictive power of big data analytics, this little data often reflects deeply sensitive information about individuals: their medical treatments and concerns; their religious practices; their sexual orientation; where they spend their time; who they communicate with, and the list goes on. This is the lesson from the now-infamous Target "pregnancy predictor" score. According to media reports, Target was able to apply an algorithm to mundane purchasing patterns, such as the

[14] *See* FED. TRADE COMM'N, PROTECTING CONSUMER PRIVACY IN AN ERA OF RAPID CHANGE: RECOMMENDATIONS FOR BUSINESSES AND POLICYMAKERS (Mar. 2012) ("FTC Privacy Report"), *available at* http://www.ftc.gov/os/2012/03/120326privacyreport.pdf.

purchase of larger quantities of unscented hand lotion, to determine that a teenager was pregnant, and to market to her with a view to her predicted delivery date in a way that alerted her father.[15]

I do not pretend that transparency and simplified notice and choice are a silver bullet. As an increasingly large number things become "smart" – our TVs, cars, and household appliances, to name just a few – even companies that seek to provide meaningful notice and choice may find it challenging to do so. But in my mind, the question is not *whether* consumers should be given a say over unexpected uses of their data; rather, the question is *how* to provide simplified notice and choice when it comes to big data. That is an issue the FTC explored at a workshop we convened last fall on the Internet of Things,[16] and on which we which we expect to issue a report later this year.

B. Data Brokers

We also need more transparency when it comes to the complex ecosystem in which consumer data is shared with entities – often called "third parties" – that operate behind the scenes. This includes data brokers. These are companies in the business of amassing information about consumers drawn from extensive online and offline sources which they aggregate and, applying powerful algorithmic tools, use to develop consumer profiles or classifications that they then sell to marketers. By their nature, data brokers operate without direct consumer interaction. As a consequence, there is little consumer awareness of their existence and little visibility into their practices.

---

[15] *See* Charles Duhigg, *How Companies Learn Your Secrets*, N.Y. TIMES (Feb. 16, 2012), *available at* http://www.nytimes.com/2012/02/19/magazine/shopping-habits.html?pagewanted=all&_r=0.

[16] Fed. Trade Comm'n, Press Release, *FTC Seeks Input on Privacy and Security Implications of the Internet of Things* (Apr. 17, 2013), *available at* http://www.ftc.gov/news-events/press-releases/2013/04/ftc-seeks-input-privacy-and-security-implications-internet-things.

In the 1970's, the Fair Credit Reporting Act or "FCRA,"[17] was enacted amidst concerns about the aggregation of consumer data by credit reporting agencies in ways that could unjustifiably limit consumers' ability to get a job, a loan, insurance, or housing. The concern today is that data brokers' products may in some cases fall outside of the FCRA, even if they impact consumers' employment, credit, insurance, or housing prospects. There is also concern that marketers of predatory or fraudulent offers may be able to target low-income or financially vulnerable consumers as a result of information obtained from data brokers.[18]

The Commission is in the midst of a study of nine data brokers.[19] We have been examining the nature and sources of the data these brokers collect; how they use, maintain, and disseminate it; and the extent to which they give consumers tools to control the use of their data. We are at the final stages of our study and expect to issue a report shortly. It is my hope that the forthcoming FTC report will spur efforts by Congress and the data broker industry for greater transparency and consumer control.

C. Discrimination by Algorithm

Big data also presents the risk of what others and I have called "discrimination by algorithm," and what the White House has called "digital redlining."[20] Big data analytics raises the possibility that facially neutral algorithms may be used to discriminate against low-income and economically vulnerable consumers. There is the worry that analytic tools will be used to exacerbate existing socio-economic disparities, by segmenting consumers with regard to the

[17] 15 U.S.C. § 1681 *et seq.*

[18] *See, e.g., United States v. Direct Lending Source, Inc.*, No. CV-2441 (S.D. Cal. filed Oct. 12, 2012) (complaint and consent order) (alleging vendor of lists of consumer purchased and resold lists of sold lists of consumers in financial distress to marketers of loan modification, debt relief, and foreclosure relief services); Charles Duhigg, *Bilking the Elderly with a Corporate Assist*, N.Y. TIMES (May 20, 2007), *available at* http://www.nytimes.com/2007/05/20/business/20tele.html?pagewanted=all&_r=0.

[19] *See* Fed. Trade Comm'n, Press Release, *FTC to Study Data Broker Industry's Collection and Use of Consumer Data* (Dec. 18, 2012), *available at* http://www.ftc.gov/opa/2012/12/databrokers.shtm.

[20] White House Big Data Report at 53.

customer service they receive, the prices they are charged, and the types of products that are marketed to them.

I welcome the White House's call for attention to this issue, which the FTC has already begun to contemplate. Last month, the FTC announced a public workshop, to take place on September 15, that will address big data as a potential tool for inclusion or exclusion of low-income and economically vulnerable consumers.[21] This workshop will build on a public roundtable we held earlier this spring to examine the proliferation of predictive scores for consumers, fueled by big data.[22] These are critical issues. As big data analytics come to affect more and more of commerce, it is vital that we be alert to them.

V. Solutions

To close, I'd like to highlight several areas where steps can be taken by a combination of policymakers, industry, and even those of you who are members of the media, to ensure that consumers can feel justifiably confident that their information will be used responsibly in a big data world.

Robust De-identification and Accountability. Effective de-identification is increasingly important in a big data world. By stripping out unique identifiers and adding statistical "noise," de-identification enables companies and researchers to spot correlations without regard to the identity of the individuals reflected in the data set. But as the FTC has recognized, de-identification isn't foolproof. There is always the possibility that de-identified data sets can be re-identified. That's why the FTC has recommended that companies robustly de-identify data,

[21] Fed. Trade Comm'n, Press Release, *FTC to Examine Effects of Big Data on Low Income and Underserved Consumers at September Workshop* (Apr. 11, 2014), *available at* http://www.ftc.gov/news-events/press-releases/2014/04/ftc-examine-effects-big-data-low-income-underserved-consumers.

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

publicly commit not to attempt to re-identify data, and contractually require the same public commitment of any service providers with which they share information.[23] I believe this approach sensibly balances the benefits and risks of de-identification. At the same time, I would like to see more work done by industry and technologists to develop better technical tools for de-identification.

Consumer Privacy Tools. The rise of big data means that technologists, policymakers, privacy advocates, and entrepreneurs should devote greater energy to developing easy and effective technological methods to give consumers greater control over their information. There is overwhelming evidence of a hunger for such tools.[24] The growth of sensing and tracking technologies means that now is the time to strengthen tools, such as do-not-track mechanisms, that give consumers a way to easily control who gets access to their data. As Latanya Sweeney, the FTC's chief technologist and Harvard professor, asked at the first White House workshop on big data, "Computer science got us into this mess; can consumer science get us out of it?"[25] The clear answer is that we have to try.

---

[23] FTC Privacy Report at 18-22.

[24] *See, e.g.*, *Consumer Confidence in Online Privacy Hits 3 Year Low*, AD WEEK (Jan. 24, 2014), *available at* http://www.adweek.com/news/technology/consumer-confidence-online-privacy-hits-3-year-low-155255; Jeff Goldman, *88 Percent of U.S. Consumers Are Worried About Data Privacy*, ESECURITY PLANET (Apr. 16, 2014), *available at* http://www.esecurityplanet.com/network-security/88-percent-of-u.s.-consumers-are-worried-about-data-privacy.html; Somini Sengupta, *Americans Go to Great Lengths to Mask Web Travels, Survey Finds*, N.Y. TIMES (Sept. 3, 2013), *available at* http://nyti.ms/19FQ7j5; Meredith Whipple, *CR Survey Finds That Most Consumers Are Still "Very Concerned" About Online Privacy*, Consumers Union Blog (Apr. 3, 2012), http://hearusnow.org/posts/1055-cr-survey-finds-that-most-consumers-are-still-very-concerned-about-online-privacy; David Sarno, *Tech Firms' Data Gathering Worries Most Californians, Poll Finds*, L.A. TIMES (Mar. 31, 2012), *available at* http://www.latimes.com/news/local/la-fi-privacy-poll-20120331,0,2763981.story; Ki Mae Heussner, *Divorcees, Southerners Most Concerned About Web Privacy, 90 Percent Of Online Adults Worry About Privacy Online, Study Shows*, AD WEEK (Feb. 12, 2012), *available at* http://www.adweek.com/news/technology/divorcees-southerners-most-concerned-about-web-privacy-138185.

[25] *See* Cameron F. Kerry, *Using Technology to Better Inform Consumers about Privacy Decisions* (Apr. 30, 2014), *available at* http://www.brookings.edu/blogs/techtank/posts/2014/04/30-privacy-for-consumers-kerry (quoting Sweeney); *see also* Video, *Big Data Privacy Workshop: Advancing the State of the Art in Technology and Practice* (Mar. 3, 2014), *available at* http://web.mit.edu/bigdata-priv/agenda.html.

The Role of the Media. Finally, the media organizations represented in this room have a vital role to play as well. In recent years, premier news organizations have paid increasing attention to consumer privacy issues, publicizing excesses in some data gathering methods. Such public scrutiny gives firms a powerful incentive to act as responsible stewards of consumer information.

*** * * ***

McKinsey, the global management consulting firm, recently cautioned its business clients that privacy has become the "third rail in the public discussion of big data," noting the media attention paid to those who disregard consumer interests in collecting and using consumer information.[26] The solution, McKinsey recognized, is to address, and not shrink from, privacy concerns.[27] The way to do this McKinsey explained, is to give consumers greater control over their information in order to build their trust.[28]

At the FTC, we also believe that consumer confidence is a prerequisite to big data and the Internet of Things realizing their full growth potential. That is among the reasons why the FTC will continue to actively use its civil enforcement authority and research and policy function in the privacy arena. We are still at the early stages of the big data age. I am confident that we can realize the benefits of our connected future while mitigating the privacy and security challenges that it brings.

Thank you.

---

[26] Brad Brown, David Court, & Tim McGuire, *Views from the Front Lines of the Data Analytics Revolution*, MCKINSEY QUARTERLY (Mar. 2014), *available at* http://www.mckinsey.com/insights/business_technology/views_from_the_front_lines_of_the_data_analytics_revolution.

[27] *See id.*

[28] *See id.*