Big Data and Consumer Trust: Progress and Continuing Challenges

U.S. Federal Trade Commissioner Julie Brill
Remarks Before the International Conference of Data Protection and Privacy Commissioners

October 15, 2014

Good afternoon. I am pleased to have the opportunity to discuss privacy and big data with this distinguished audience, and I am particularly delighted to be part of a plenary session with my dear friends Peter Hustinx and Jacob Kohnstamm. I would also like to thank the Government of Mauritius and Commissioner Madhub for being such gracious hosts.

I'd like to talk to you this morning about the benefits and challenges of big data. I believe we are starting to realize some of the benefits of bringing more data to bear on our major social challenges. In the healthcare sector, doctors have used big data to determine when premature babies are likely to develop an infection,[1] and software developers have created mobile apps that distribute information to clinicians about the types of bacteria and their resistance patterns in different geographical areas.[2] Connected refrigerators and other home appliances are starting to provide convenience and, at the same time, reduce energy consumption and cost.[3] Big data promises to address other important societal issues like keeping kids in high school;[4] and providing first responders in crisis situations with real-time information about the injured or those who lack power, water, or food.[5] And in the near future, connected and driverless cars may make the roadways safer for all of us as older drivers – like my 86-year-old mother – experience a reduction in their safe driving capabilities.[6]

---

[1] Brian Proffitt, *Big Data Analytics May Detect Infections Before Clinicians*, ITWORLD (Apr. 12, 2012, 3:36 PM), *available at* http://www.itworld.com/big-datahadoop/267396/big-data-analytics-may-detect-infection-clinicians.

[2] *See* Jennifer Bresnick, *Big Data Helps Tackle Drug Resistance at the Point of Care*, HEALTH IT ANALYTICS (Oct. 3, 2013), *available at* http://healthitanalytics.com/2013/10/03/big-data-helps-tackle-drug-resistance-at-the-point-of-care/ (discussing the Bugs + Drugs app, which "provides physicians with a way to track antibiotic resistance patterns based on the communities they serve, using geolocation data, medication prescriptions, and patient outcome information to spot superbugs before they take lives").

[3] *See, e.g.*, Megan Wallerton, *Smart Appliances, Connected Homes at CES 2014*, CNET (Jan. 10, 2014, 10:48 AM), *available at* http://ces.cnet.com/8301-35306_1-57616968/smart-appliances-connected-homes-at-ces-2014/.

[4] *See* Centre for Information Policy Leadership, *Big Data and Analytics: Seeking Foundations for Effective Privacy Guidance* 6-7 (Feb. 2013), *available at* http://www.hunton.com/files/Uploads/Documents/News_files/Big_Data_and_Analytics_February_2013.pdf (discussing efforts to reduce the high school drop-out rate using student record analysis in Mobile County, Alabama).

[5] *See* Lisa Wirthman, *How First Responders Are Using Big Data to Save Lives*, FORBES BRANDVOICE (Jan. 10, 2014, 12:02 PM), *available at* http://www.forbes.com/sites/emc/2014/01/10/how-first-responders-are-using-big-data-to-save-lives/#.

[6] *See* Nat'l Highway Transp. Safety Admin., U.S. Department of Transportation Issues Advance Notice of Rulemaking to Begin Implementation of Vehicle-to-Vehicle Communications Technology (Aug. 18, 2014), *available at* http://www.nhtsa.gov/About+NHTSA/Press+Releases/NHTSA-issues-advanced-notice-of-proposed-

But I also believe that big data will not realize its full potential unless companies, researchers and policymakers work to build consumer trust in the big data enterprise.[7] As in the past, privacy and data security protections will continue to play an essential role in building consumer trust. The question is how to put those protections into practice. My agency, the Federal Trade Commission (FTC), has been actively engaged in answering this question through a series of public workshops and reports.[8]

Our counterparts around the world are asking the same question through similar efforts. The European Commission's recently released Communication on a data-driven economy;[9] the UK Information Commissioner's Office (ICO) recent report on big data and data protection;[10] the OECD's Global Forum on the Knowledge Economy;[11] and Japan's review of its own data privacy law in light of big data's challenges – these are just some examples of the common search by regulators, businesses, and others for answers about how to reconcile the furious pace of growth in big data analytics with more stable values such as privacy and fair treatment.

I find it encouraging that all of us – with our diverse perspectives and legal systems – are affirming the relevance of fundamental privacy principles in the big data era, and are focusing our attention on *how* the principles apply in our data-intensive world.

The Main Challenges to Consumer Trust: Data Security, Sensitive Information Protection, and Ethical Data Practices

Let me focus on three challenges to building consumer trust and realizing big data's full social and economic potential.

---

rulemaking-on-V2V-communications (stating results of preliminary report on Left Turn Assist and Intersection Movement Assist technologies, which estimates that the technologies could prevent up to 592,000 crashes and save 1,083 lives per year).

[7] For a full elaboration of this argument, see generally Julie Brill, Comm'r, FTC, Keynote Address at the U.S. Chamber of Commerce Foundation Conference on the Future of Data-Driven Innovation: The Trees and the Forest: Protecting Consumer Trust in the Big Data Era (Oct. 7, 2014), *available at* http://www.ftc.gov/system/files/documents/public_statements/590171/141007uschamberbrillremarks.pdf.

[8] *See, e.g.*, FTC, Internet of Things Workshop – Privacy and Security in a Connected World (last visited Oct. 9, 2014), http://www.ftc.gov/news-events/events-calendar/2013/11/internet-things-privacy-security-connected-world; FTC, Big Data: A Tool for Inclusion or Exclusion (last visited Oct. 9, 2014), http://www.ftc.gov/news-events/events-calendar/2014/09/big-data-tool-inclusion-or-exclusion.

[9] Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee, and the Committee of the Regions, *Towards a Thriving Data-Driven Economy* (July 2, 2014), *available at* https://ec.europa.eu/digital-agenda/en/news/communication-data-driven-economy.

[10] UK INFORMATION COMMISSIONER'S OFFICE, BIG DATA AND DATA PROTECTION (July 28, 2014, v. 1.0), *available at* http://ico.org.uk/news/latest_news/2014/~/media/documents/library/Data_Protection/Practical_application/big-data-and-data-protection.pdf.

[11] OECD, Global Forum on the Knowledge Economy (last visited Oct. 9, 2014), http://www.oecd.org/innovation/inno/globalforumontheknowledgeeconomy.htm.

Data Security

I will begin with data security, which has been a priority of the FTC for more than a decade, in part because we continue to see one massive data breach after another putting consumers' identities and financial interests at risk.[12] Data security is also an FTC priority because, quite simply, there is no privacy without appropriate data security. In recent years, we have made it clear that data breaches involving financial information,[13] as well as unexpected revelations about our health,[14] our families,[15] our location,[16] or activities in our homes,[17] can cause substantial harm to consumers.[18]

And now we are starting to discover that vulnerabilities in connected devices can also reveal highly sensitive information. This was precisely the issue in the FTC's first enforcement action involving the Internet of Things, which was based on our allegation that a company's lax

---

[12] *See, e.g.*, Jessica Silver-Greenberg, Matthew Goldstein, and Nicole Perlroth, *JPMorgan Chase Hacking Affects 76 Million Households*, N.Y. TIMES DEALBOOK (Oct. 2, 2014, 12:50 PM), *available at* http://dealbook.nytimes.com/2014/10/02/jpmorgan-discovers-further-cyber-security-issues/; Robin Seidl, *Home Depot's 56 Million Card Breach Bigger Than Target's*, WALL ST. J. (last updated Sept. 18, 2014, 5:43 PM), *available at* http://online.wsj.com/articles/home-depot-breach-bigger-than-targets-1411073571; Brian Krebs, *The Target Breach, by the Numbers*, KREBS ON SECURITY (May 6, 2014), *available at* http://krebsonsecurity.com/2014/05/the-target-breach-by-the-numbers/.

[13] *See, e.g.*, The TJX Cos., Inc., No. C-4227 (F.T.C. July 29, 2008) (consent order), *available at* http://www.ftc.gov/enforcement/cases-and-proceedings/cases/2008/08/tjx-companies-inc-matter; Dave & Buster's, Inc., No. C-4291 (F.T.C. May 20, 2010) (consent order), *available at* http://www.ftc.gov/enforcement/cases-and-proceedings/cases/2010/06/dave-busters-incin-matter; DSW, Inc., No. C-4157 (F.T.C. Mar. 7, 2006) (consent order), *available at* http://www.ftc.gov/enforcement/cases-and-proceedings/cases/2006/03/dsw-incin-matter; *BJ's Wholesale Club, Inc.*, No. C-4148 (F.T.C. Sept. 20, 2005) (consent order), *available at* http://www.ftc.gov/enforcement/cases-and-proceedings/cases/2005/09/bjs-wholesale-club-inc-matter.

[14] *See* GMR Transcription Servs., No. C-4482 (F.T.C. Aug.14, 2014) (consent order), *available at* http://www.ftc.gov/system/files/documents/cases/140821gmrdo.pdf; CBR Sys., Inc., No. C-4400 (F.T.C. Apr. 29, 2013) (consent order), *available at* http://www.ftc.gov/sites/default/files/documents/cases/2013/05/130503cbrdo.pdf.

[15] *See* TRENDnet Inc., No. C-4426, 2014 WL 556262 (F.T.C. Jan. 16, 2014) (consent order), *available at* http://www.ftc.gov/system/files/documents/cases/140207trendnetdo.pdf.

[16] *See* FTC, PROTECTING CONSUMER PRIVACY IN AN ERA OF RAPID CHANGE: RECOMMENDATIONS FOR BUSINESSES AND POLICYMAKERS 58–59 (2012), *available at* http://www.ftc.gov/sites/default/files/documents/reports/federal-trade-commission-report-protecting-consumer-privacy-era-rapid-change-recommendations/120326privacyreport.pdf (stating that "individualized location data is sensitive").; Goldenshores Techs., LLC, No. C-4446, at ¶ 7 (F.T.C. Mar. 31, 2014) (complaint), *available at* http://www.ftc.gov/system/files/documents/cases/140409goldenshorescmpt.pdf (alleging that location information is sensitive); *id.* (consent order), *available at* http://www.ftc.gov/system/files/documents/cases/140409goldenshoresdo.pdf.

[17] *See TRENDNet*, *supra* note 15.

[18] The FTC has recognized this broader set of privacy harms in cases that do not involve security breaches. *See, e.g.*, Aaron's, Inc., No. C-4442 (F.T.C. Mar. 10, 2014), *available at* http://www.ftc.gov/system/files/documents/cases/140311aaronsdo.pdf; DesignerWare, LLC, No. C-4390 (F.T.C. Apr. 11, 2013), *available at* http://www.ftc.gov/sites/default/files/documents/cases/2013/04/130415designerwaredo.pdf.

security practices led to live feeds from Internet-connected home video cameras being hijacked and posted to public Internet sites.[19]

Looking more broadly, a recent study by Hewlett-Packard found that 90 percent of connected devices are collecting personal information, and 70 percent of them are transmitting this data without encryption.[20] As more devices become connected to the Internet, the potential grows for more information about the most intimate details of our lives to slip into the wrong hands – and to leave other consumer devices and accounts vulnerable – unless appropriate security safeguards are put into place.

Improving security of data that is personally identifiable or linkable to individuals is a must. While some are enthusiastic about indiscriminately collecting data now and sorting it out later, I see big security risks in this approach. A better approach – and one that is consistent with the FTC's view that risk assessments and data minimization are integral to reasonable data security practices – is for companies to take a close look at what data they have and what data they actually need to serve their customers.[21] And wherever possible, companies should robustly deidentify this data, and promise to not reidentify it.[22]

Sensitive Information

A second challenge to consumer trust comes from the collection and use of sensitive personal information. Today I will focus on health information, because it presents both some of the greatest opportunities and some of the greatest risks. Some of the most exciting prospects for society-changing innovations come from wearable devices and mobile apps that encourage consumers to collect and store their own health data. Yet much of this information – some of it highly sensitive – falls outside the current boundaries of U.S. law.[23]

---

[19] *See* FTC, Press Release, FTC Approves Final Order Settling Charges Against TRENDNet, Inc. (Feb. 7, 2014), *available at* http://www.ftc.gov/news-events/press-releases/2014/02/ftc-approves-final-order-settling-charges-against-trendnet-inc.

[20] Hewlett-Packard, *Internet of Things Research Study* 2 (July 2014), *available at* http://h20195.www2.hp.com/V2/GetDocument.aspx?docname=4AA5-4759ENW&cc=us&lc=en.

[21] *See* FTC, Prepared Statement on Protecting Personal Consumer Information from Cyber Attacks and Data Breaches Before the Senate Committee on Commerce, Science, and Transportation 9 (Mar. 26, 2014), *available at* http://www.ftc.gov/system/files/documents/public_statements/293861/140326datasecurity.pdf.

[22] *See* FTC, PROTECTING CONSUMER PRIVACY IN AN ERA OF RAPID CHANGE: RECOMMENDATIONS FOR BUSINESSES AND POLICYMAKERS 21-22 (2012), *available at* http://www.ftc.gov/sites/default/files/documents/reports/federal-trade-commission-report-protecting-consumer-privacy-era-rapid-change-recommendations/120326privacyreport.pdf.

[23] *See, e.g.*, Comments of Joy Pritts, Transcript of the FTC Seminar on User Generated and User Controlled Health Data 35-36 (May 7, 2014), *available at* http://www.ftc.gov/system/files/documents/public_events/195411/2014_05_07_consumer-generated-controlled-health-data-final-transcript.pdf (stating that "[w]e are trying to move from a paradigm in where health care is just provided on an episodic basis and really treat the patient more holistically" but "[w]hat happens then is . . . we are actively encouraging people to move their information potentially out of a HIPAA-protected bubble into the hands of others who may not be subjected to HIPAA").

Companies should give consumers great control over collection and use of sensitive data like health information. Meaningful individual control is a much broader concept than simply permitting or refusing information collection at one point in time.[24] Instead, companies should develop intuitive and immersive consumer dashboards, apps and other tools that will engage and, at the same time, inform consumers about how their sensitive health information is being collected and used.[25] And to the extent that this sensitive information winds up in data broker profiles, data brokers must similarly empower consumers with an easy-to-use portal that will give them the ability to keep aspects of their private lives away from big data driven marketing.[26]

Discrimination and Unethical Data Practices

The third challenge to consumer trust that I want to highlight comes from the possibility of unfair or unethical treatment as companies use increasingly powerful analytics tools on the massive amounts of data that are available about individual consumers. This is a challenge that *all* companies need to take seriously.

Some of the findings in the FTC's ground-breaking study on data brokers, released earlier this year, raised this issue. We found that the profiles these companies create about individuals, which may contain thousands of data points,[27] will sometimes separate consumers according to race, ethnicity, family status, and other characteristics that companies are not allowed to consider for purposes such as housing, credit, employment, and medical care.[28]

In the marketing context that these profiles are intended to serve, merely collecting such information might not present a legal problem under current U.S. law. Indeed, these and other big data tools have the potential to promote economic inclusion. For example, big data driven marketing can make underserved consumers aware of opportunities for credit and other services.[29]

---

[24] *See generally* Julie Brill, Comm'r, FTC, Sloan Cyber Security Lecture: A Call to Arms: The Role of Technologists in Protecting Privacy in the Age of Big Data (Oct. 23, 2013), *available at* http://www.ftc.gov/sites/default/files/documents/public_statements/call-arms-role-technologists-protecting-privacy-age-big-data/131023nyupolysloanlecture.pdf; Julie Brill, Comm'r, FTC, Keynote Address at the 23rd Computers, Freedom, and Privacy Conference: Reclaim Your Name (June 26, 2013), *available at* http://www.ftc.gov/sites/default/files/documents/public_statements/reclaim-your-name/130626computersfreedom.pdf.

[25] *See* Brill, A Call to Arms, *supra* note 24, at 4-5.

[26] *See id* at 9-10 *and* Brill, Reclaim Your Name, *supra* note 24, at 10-11. *See also* FTC, DATA BROKERS: A CALL FOR TRANSPARENCY AND ACCOUNTABILITY iv (2014), *available at* http://www.ftc.gov/system/files/documents/reports/data-brokers-call-transparency-accountability-report-federal-trade-commission-may-2014/140527databrokerreport.pdf; EXEC. OFFICE OF THE PRESIDENT, BIG DATA: SEIZING OPPORTUNITIES, PRESERVING VALUES 62 (2014), *available at* http://www.whitehouse.gov/sites/default/files/docs/big_data_privacy_report_may_1_2014.pdf.

[27] *See* FTC, DATA BROKERS, *supra* note 26, at (reporting that one data broker has "3000 data segments for nearly every consumer").

[28] *See id.* at 20 n.52.

[29] *See* FTC, Conference Description, Big Data: A Tool for Inclusion or Exclusion?, http://www.ftc.gov/news-events/events-calendar/2014/09/big-data-tool-inclusion-or-exclusion (last visited Oct. 14, 2014) ("[U]ses of big data

But there is also a clear potential for use of the information to be harmful and discriminatory, and to destroy consumer trust. The same data that allows banks to reach traditionally unbanked, financially vulnerable populations could just as easily be used to target them with advertisements for high-interest payday loans.[30]

Moreover, consumer segments that steer clear of traditionally restricted categories could still have devastating emotional effects on consumers. Consider, for example, a list of domestic abuse victims. Such a list might be useful for companies that want to market home security devices. But I think this is a case in which the explanation that the list is "just for marketing" falls short. We all need to discuss the many issues surrounding consumer profiles like these, including the individual data elements that they contain, how they group consumers together, and how the profiles are used in practice.

And as companies begin scrutinizing their own data –perhaps supplementing it with information from data brokers – they also need to be on the lookout for how data can lead them into making distinctions that are ethically, if not legally, questionable. For example, what if a company analyzing its own data, in an effort to identify "good" versus "troublesome" customers, ends up tracking individuals along racial or ethnic lines? A recent *Harvard Business Review* article argues that this kind of result isn't just possible but inevitable, and all companies should think carefully about where "value-added personalization and segmentation end[s] and harmful discrimination begin[s]."[31]

Much of the challenge in ethical data practices lies behind the scenes, out of consumers' view. Therefore, more of the burden is on companies to ensure that their collection and use practices are consistent with a trusted relationship. I encourage companies to think about this the way engineers think about designing automobiles: while we want to give consumers better control and transparency tools that they can easily access on their dashboards, we must also ensure that companies build better protections "under the hood" to ensure ethical treatment of consumers.[32]

---

are expected to create efficiencies, lower costs, and improve the ability of certain populations to find and access credit and other services."). *See also* Comment of the Chamber of Commerce of the United States on the Big Data: A Tool for Inclusion or Exclusion? Workshop 3 (Aug. 15, 2014), *available at* http://www.ftc.gov/system/files/documents/public_comments/2014/08/00021-92389.pdf (quoting with approval the FTC's conference description).

[30] *See, e.g.*, Comment of the National Consumer Law Center on the Big Data: A Tool for Inclusion or Exclusion? Workshop 2 (Aug. 15, 2014), *available at* http://www.ftc.gov/system/files/documents/public_comments/2014/08/00018-92374.pdf; Jeffrey Chester and Edmund Mierzwinski, Big Data Means Big Opportunities and Big Challenges: Promoting Financial Inclusion and Consumer Protection in the "Big Data" Financial Era 13 (Mar. 2014) (submitted as a comment of the Center for Digital Democracy and U.S. PIRG on the Big Data: A Tool for Inclusion or Exclusion? Workshop), *available at* http://www.ftc.gov/system/files/documents/public_comments/2014/05/00003-90097.pdf.

[31] Michael Schrage, *Big Data's Dangerous New Era of Discrimination*, HARVARD BUSINESS REVIEW BLOG NETWORK (Jan. 29, 2014, 8:00 a.m.), http://blogs.hbr.org/2014/01/big-datas-dangerous-new-era-of-discrimination/.

[32] Yochi Dreazen, . . . *Guard Your Privacy: Steps to Protect Confidentiality While Online Are Often Underused*, WALL ST. J. (Nov. 18, 2002, 9:52 AM), *available at* http://online.wsj.com/articles/SB10372223183106966668 (quoting Marc Rotenberg as saying, "I don't think users need more settings on the dashboard – they need online privacy protections under the hood.").

Data brokers should take a strong, proactive step by assessing the potential impact of their products that profile consumers by race, ethnicity or other sensitive classifications, or that are proxies for such sensitive classifications.

And companies that are beginning to dive into their own data should deploy greater resources and imagination to designing intuitive portals, dashboards, and better interfaces for consumers to use to control their privacy and security. Companies could also make ethics reviews part of their big data analytics business practices – perhaps by creating "consumer subject review boards" to identify and reduce consumer risks, as one U.S. privacy scholar has suggested.[33] And whether or not companies go to this level of formality, every one of them should be asking whether their analysis of consumer data is taking them into questionable territory.[34]

* * * * * *

The fundamental privacy principles that many of us hold and enforce have proven over years and decades that they are durable and capture important attributes of individual freedom and autonomy. The rise of big data is only the most recent challenge to these principles, and many of us here have concluded that traditional privacy principles can not only coexist with big data, but can also improve big data's chances for success. For those of us who care deeply about privacy, affirming these principles will not be enough. We will need to continue to examine specific big data challenges – like data security, sensitive information, and discrimination – and get specific about solutions.

Thank you.

[33] *See generally* Ryan Calo, *Consumer Subject Review Boards: A Thought Experiment*, 66 STAN. L. REV. ONLINE 97 (Sept. 3, 2013), *available at* http://www.stanfordlawreview.org/online/privacy-and-big-data/consumer-subject-review-boards.

[34] *See* Schrage, *Big Data's Dangerous New Era of Discrimination*, *supra* note 31.