Commissioner Julie Brill's Keynote Address
Joint USCIB/BIAC/OECD Conference on "Growth, Jobs, & Prosperity in the Digital Age: OECD Shapes the Policy Environment"
March 10, 2014

Thank you, Joe Alhadeff, for that kind introduction, and to USCIB, BIAC, and the OECD for inviting me to speak today. I always look forward to the opportunity to discuss important privacy issues with my colleagues from around the globe.

Technology is transforming our lives. Its enormous benefits have become part of our daily routine. We use Google Maps to help us find our destinations, we search for medical information on WebMD, we manage our finances on mint.com, and we post selfies on Twitter.

But these now-familiar services are just the beginning of our connected future. Our cars are computers with wheels, wearable medical devices notify others when we are ill, and our connected refrigerator will soon tell us that we've had a sufficient amount of beer for one night. These transformative online and mobile experiences collectively yield an enormous amount of data about us. In a real sense, we are becoming the sum of our digital parts.

The estimates of the data we collectively generate are staggering. One estimate, already more than two years out of date, suggests that 1.8 trillion gigabytes of data were created in the year 2011 alone – that's the equivalent of every U.S. citizen writing three tweets per minute for almost 27,000 years.[1]

This gold mine of data can be put to important, even transformative uses. We are all familiar with big data's ability to personalize our daily activities – helping companies determine which ads to pitch to us, which newspaper articles to recommend, and which movie should be next in our queue. But big data analytics promises to bring us more profound societal benefits like keeping kids in high school;[2] improving energy efficiency to help conserve our natural resources;[3] providing first responders in crisis situations with real-time information about the injured or those who lack power, water, or food;[4] and performing other miracles in the health

[1] Lucas Mearian, *World's data will grow by 50X in next decade, IDC study predicts*, COMPUTERWORLD, June 28, 2011, *available at* http://www.computerworld.com/s/ article/9217988/ World_s_data_will_grow_by_50X_in_next_decade_IDC_study_predicts?pageNumber=1.

[2] Centre for Information Policy Leadership, *Big Data and Analytics: Seeking Foundations for Effective Privacy Guidance*, at 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).

[3] *See* Omer Tene & Jules Polonetsky, *Big Data for All: Privacy and User Control in the Age of Analytics*, 11 NW. J. TECH. & INTELL. PROP. 239 (2013).

[4] *See* 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/#.

care sector, such as preventing infections in premature children[5] and predicting disease outbreaks.[6]

The global transfer of data can magnify this potential and produce revolutionary economic and societal benefits. Some of the most striking benefits could come to developing countries. For example, Dr. Sugata Mitra, an educational researcher, conducted an experiment by placing a computer in a low-income area in India, without any instructions, for children to use.[7] He found that the children, who only spoke local Indian languages and had never seen a computer before, quickly became adept at using this technology, browsed the Internet, and in a similar experiment, began learning complex biotechnology principles—in English.[8] He concluded that self-organized learning could have a tremendous impact on global education, and outlined his hope for "a school in the cloud," which would use cloud-based services to facilitate self-organized learning.[9]

We are all eager to reap these and other potential benefits of innovative data flows and new technologies. Yet consumers, policy makers, and academics also see risks posed by big data analytics and the vast storehouses of data it yields. Most of us have been loath to examine too closely the price we pay by forfeiting control of our personal data in exchange for the convenience, ease of communication, and fun in a free-ranging and mostly free cyberspace.

As we further examine the privacy implications of big data analytics, I believe one of the most troubling practices that we need to address is the collection and use of data — whether generated online or offline — to make sensitive predictions about consumers, such as those involving their health conditions, financial condition, sexual orientation, and race.

Let's look at a well-known, and by now infamous, example. Before Target made news for a data security breach that may involve 110 million consumers' credit cards and debit cards, the company received a lot of attention for its big-data-driven campaign to identify pregnant customers through an analysis of consumers' purchases at its stores, a so-called "pregnancy predictor score."[10] Target was able to calculate, not only *whether* a consumer was pregnant, but

---

[5] 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*.

[6] *See* Sue Poremba, *Can Big Data And Mobile Make Health Care More Effective?*, FORBES EMCVOICE, Jan. 22, 2014, *available at* http://www.forbes.com/sites/emc/2014/01/22/can-big-data-and-mobile-make-health-care-more-effective/ (discussing the use of big data to predict individuals' health status and guide preventative health programs).

[7] *See* Sugata Mitra, Build a School in the Cloud, TED talk, *available at* *http://www.npr.org/2013/06/21/179015266/how-much-can-children-teach-themselves*. *See also* http://www.npr.org/templates/transcript/transcript.php?storyId=179015266.

[8] *See id.*

[9] *See id.*

[10] *See* Charles Duhigg, *How Companies Learn Your Secrets*, N.Y. TIMES , Feb. 16, 2012, *available at* http://www.washingtonpost.com/blogs/the-switch/wp/2014/01/17/yes-google-glass-users-look-weird-but-googles-smart-contact-lens-will-change-all-that/.

also *when* her baby was due.[11] It used the information to win the expectant mom's loyalty by offering coupons tailored to her stage of pregnancy.[12]

To be clear, I don't have any information indicating that Target sold its pregnancy predictor score or lists of pregnant customers to third parties, or that doing so would have violated the law. Yet there are companies that develop algorithms that predict other health conditions – diabetes, cancer, mental illness – based on store purchases, social media posts, and other seemingly innocuous activities, and sell that information to marketers and others.[13] All of this creation, analysis, and use of consumers' health information happens outside of HIPAA – outside the US regulatory regime designed to protect health information.

I believe we should all be concerned about the use of deeply sensitive personal information to make decisions about consumers outside a legal regime that would provide notice and an opportunity to challenge the accuracy of the data. Similarly, we should be concerned about the risk that such sensitive personal information may fall into the wrong hands through a data breach. But more fundamentally, I believe we should be concerned about the damage that is done to our sense of privacy and autonomy in a society in which information about some of the most sensitive aspects of our lives is available for analysts to examine without our knowledge or consent, and for anyone to buy if they are willing to pay the going price.

These concerns, of course, are not limited to the world of commercial data brokers. We don't have to pass judgment on the revelations about the NSA and other intelligence agencies' data collection and use practices to acknowledge that the recent disclosures have sparked a necessary and overdue debate on how to balance national security against citizens' privacy rights. For those of us who have been looking at the issue of privacy in the Internet age for many years, there is a further benefit: consumers are now more aware than ever of how much their personal data is free-floating in cyberspace, ripe for any data miner – government or otherwise – to collect, package, use – and on the commercial side – sell.

But with that knowledge comes power – the power to review, this time with eyes wide open, what privacy means – or should mean – in the age of the Internet. I believe that's what President Obama meant in June, and again last month, when he noted that the "challenges to our

---

[11] *See id.*

[12] *See id.*

[13] *See* U.S. GOVERNMENT ACCOUNTABILITY OFFICE, REPORT TO THE CHAIRMAN, COMMITTEE ON COMMERCE, SCIENCE, AND TRANSPORTATION, U.S. SENATE, INFORMATION RESELLERS CONSUMER PRIVACY FRAMEWORK NEEDS TO REFLECT CHANGES IN TECHNOLOGY AND THE MARKETPLACE 53 (2013). The U.S. Senate Commerce Committee staff describes another data broker that keeps 75,000 data elements about consumers in its system, including the use of yeast infection products, laxatives, and OB/GYN services, among other health-related data. *See* STAFF OF S. COMM. ON COMMERCE, SCIENCE, AND TRANSP., 113TH CONG., A REVIEW OF THE DATA BROKER INDUSTRY: COLLECTION, USE, AND SALE OF CONSUMER DATA FOR MARKETING PURPOSES 12, 14 (2013) (citing documentary submission from Equifax and listing health care-related data elements that Equifax maintains) [hereinafter "DATA BROKER REPORT"]. And the Wall Street Journal recently informed us about a company that analyzes innocuous data from social media and the like to predict disease conditions like diabetes, obesity, and arthritis in order to persuade particular consumers to join medical trials. *See* Joseph Walker, *Data Mining to Recruit Sick People*, WALL ST. J, Dec. 17, 2013, *available at* http://online.wsj.com/news/article_email/SB10001424052702303722104579240140554518458-lMyQjAxMTA0MDAwNjEwNDYyWj.

privacy do not come from government alone. Corporations of all shapes and sizes track what you buy, store and analyze our data and use it for commercial purposes,"[14] and when he called for a "national conversation…about…the general problem of … big data sets, because this is not going to be restricted to government entities."[15]

Leaders within the business community have joined the President in recognizing that rebuilding the trust of individuals is essential to the success of all programs and services – both governmental and commercial – built on big data analytics.[16] These business leaders have urged companies to adopt enhanced privacy protections as a key part of strengthening consumer trust.

I agree. While I firmly believe that the national security issues must be addressed separately from the commercial privacy issues, I also firmly believe that the promise of big data – the huge benefits that we may reap from appropriately tailored use of big data analytics – will not be reached until society addresses some of the key consumer privacy concerns stemming from the creation, collection and use of sensitive consumer data and profiles.

I'd like to highlight five steps that I believe should be taken by policy makers and industry in the commercial sphere to restore consumer trust and create an ecosystem in which big data can reach its full potential.

1. Focus on Deidentification

We must encourage companies to deidentify the data they collect whenever feasible. Of course, merely stripping identifiers such as names and addresses is not sufficient; it is too easy to re-identify data.[17] My agency, the Federal Trade Commission, has developed best practices

---

[14] *See* Transcript of President Obama's Jan. 17 speech on NSA Reforms, Jan. 17, 2014, *available at* http://www.washingtonpost.com/politics/full-text-of-president-obamas-jan-17-speech-on-nsa-reforms/2014/01/17/fa33590a-7f8c-11e3-9556-4a4bf7bcbd84_story.html.

[15] *See* Devin Dwyer, *Obama to Convene Privacy, Civil Liberties Board*, June 21, 2013, *http://abcnews.go.com/blogs/politics/2013/06/obama-to-convene-privacy-civil-liberties-board/*.

[16] *See* Brad Smith, Time for an International Convention on Government Access to Data, Microsoft on the Issues (Jan. 20, 2014), *available at* http://blogs.technet.com/b/microsoft_on_the_issues/archive/2014/01/20/time-for-an-international-convention-on-government-access-to-data.aspx (advocating international treaty to provide consistent privacy protections for personal data with respect to government collection of data); Martin Sorrell, "Data, American Manufacturing, and Chinese Innovation: 5 Predictions for 2014 Economy, THE WORLDPOST, Jan. 21, 2014, *available at* http://www.huffingtonpost.com/sir-martin-sorrell/world-economic-forum-davos-2014_b_4639464.html (noting that "the spying and phone-tapping allegations can only intensify [the public's] concerns and further erode trust between individuals and organisations on the subject of personal data" and that "[b]usinesses, like governments, are going to have to work harder to show the benefits that 'big data' brings to consumers and economies, to educate the public about how that data is handled, and to demonstrate that companies are responsible custodians of people's information").

[17] In an analysis published in *Scientific Reports*, researchers found that they could recognize a specific individual with 95 percent accuracy by looking at only four points of so-called "mobility data" tracked by recording the pings cell phones send to towers when we make calls or send texts. *See* Yves-Alexandre de Montjoye, et. al., *Unique in the Crowd: The Privacy Bounds of Human Mobility*, 3 SCI REP. 1376 (2013). NSF-funded research by Alessandro Acquisti has shown that, using publicly available online data and off-the-shelf facial recognition technology, it is possible to predict – with an alarming level of accuracy – identifying information as private as an individual's social security number from an anonymous snapshot. Alessandro Acquisti and Ralph Gross, *Predicting Social Security Numbers from Public Data*, 106 PROCEEDINGS OF THE NATIONAL ACADEMIES OF SCIENCE 10975 (2009), *available at* http://www.pnas.org/content/106/27/10975.full.pdf+html.

around deidentification that strike an appropriate balance and include both robust deidentification technologies and social agreements to not reassociate deidentified data with particular individuals. This means that companies should do everything technically possible to strip their data of identifying markers; they should make a public commitment not to try to re-identify the data; and they should contractually prohibit downstream recipients from doing the same.[18]

Although robust deidentification would help, it will not solve the problem of big data profiling. The entire data broker enterprise seeks to develop greater insight into the activities, status, beliefs, and preferences of *individuals*. The data the industry employs are therefore about or linkable to individuals.[19]

2. Create Institutional Ethical Monitoring

We must also support the creation of entities and structures that appropriately monitor the ethical use of data. One proposal calls for the creation of "Consumer Subject Review Boards" to determine whether particular projects using consumer data are both legal and ethical.[20] Another proposal calls for individual companies to appoint "algorithmists" –licensed professionals who would have ethical responsibilities for an organization's appropriate handling of consumer data.[21] Ethically trained computer scientists, algorithmists, and Consumer Subject Review Boards might all have an important role to play. But we should recognize that they will only thrive in firms that thoroughly embrace "privacy by design" – from the engineers and programmers all the way up to the C-suite – firms that understand the legal and ethical dimensions of the use of algorithms to make decisions about individuals.

3. Change the Law

Changing the law would also help. We have pretty good laws in the US governing commercial privacy, and we have excellent enforcement. The Federal Trade Commission – the leading privacy regulator in the United States – has built a robust data protection and privacy enforcement program that focuses on the evolving digital and mobile marketplace.[22] The FTC

---

[18] *See* FED TRADE COMM'N, PROTECTING CONSUMER PRIVACY IN AN ERA OF RAPID CHANGE: RECOMMENDATIONS FOR BUSINESSES AND POLICYMAEKRS 21 (2012), *available at* http://www.ftc.gov/os/2012/03/120326privacyreport.pdf.

[19] *See* John Deighton & Peter Johnson, *The Value of Data: Consequences for Insight, Innovation & Efficiency in the U.S. Economy* (DMA Data-Driven Marketing Institute, Oct. 8, 2013), *available at* http://ddminstitute.thedma.org/#valueofdata.

[20] *See* Ryan Calo, *Consumer Subject Review Boards*, 66 STAN. L. REV. ONLINE 97 (2013), *available at* http://www.stanfordlawreview.org/online/privacy-and-big-data/consumer-subject-review-boards; Jules Polonetsky, Omer Tene, & Christopher Wolf, *How to Solve the President's Big Data Challenge*, IAPP Privacy Perspectives, Jan. 31, 2014, *available at* https://www.privacyassociation.org/privacy_perspectives/post/how_to_solve_the_presidents_big_data_challenge.

[21] *See* VIKTOR MAYER-SCHÖNBERGER & KENNETH CUKIER, BIG DATA: THE REVEOLUTION THAT WILL TRANSFORM HOW WE LIVE, WORK, AND THINK 180 – 182 (2013).

[22] *See, e.g.*, 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); In the Matter of Twitter, Inc., FTC File No. 092 3093 (March 3, 2011), *available at* http://www.ftc.gov/os/caselist/0923093/110311twitterdo.pdf (decision and order); In the Matter of HTC, Inc., FTC

uses its authority to stop unfair or deceptive practices that violate consumers' privacy or place consumers' data at risk.[23] We also enforce laws that protect consumers' financial[24] and health[25] information, information about children,[26] and information used to make decisions about credit, insurance, employment, and housing.[27] We also engage in rigorous data security enforcement.

Yet I believe we need to improve our commercial privacy laws in the US. I believe Congress should enact three pieces of legislation to help address these issues: (1) data broker legislation that would require data brokers to provide notice, access, and correction rights to consumers scaled to the sensitivity and use of the data at issue – and I was glad to see that Senate Commerce Committee Chairman Rockefeller and Senator Markey of Massachusetts recently introduced such a bill[28]; (2) baseline privacy legislation for the commercial arena; and (3) data security legislation.

4. Reclaim Your Name

But we need action now to address consumers' loss of control over their most private and sensitive information, even before legislation is enacted. Industry should work to enhance consumer trust by providing practical tools to consumers so they can understand more about data collection and use, and exercise appropriate control. To this end, I have started a comprehensive initiative – "Reclaim Your Name".[29] Put simply, Reclaim Your Name would give consumers more control over decisions like how much to share, with whom, and for what purpose – to reclaim their names.

File No. 122 3049 (June 25, 2013), *available at* http://www.ftc.gov/os/caselist/1223049/130702htcdo.pdf (decision and order).

[23] 15 U.S.C. §45(a).

[24] Gramm-Leach-Bliley Act of 1999, Pub. L. No. 106-102, 113 Stat. 1338 (codified in scattered sections of 12 and 15 U.S.C.).

[25] Health Insurance Portability and Accountability Act of 1996, Pub. L. 104-191, 110 Stat. 1936 (codified as amended in scattered sections of 18, 26, 29 & 42 U.S.C.); Health Information Technology for Economic and Clinical Health Act of 2009, 42 U.S.C. 300jj et seq. §§17901 et seq.

[26] Children's Online Privacy Protection Act of 1998, Pub. L. 105-277, 112 Stat. 2581-728 (codified as amended at 15 U.S.C. §§ 6501-6505).

[27] Fair Credit Reporting Act of 1970, Pub. L. No. 91-508, 84 Stat. 1128 (codified as amended at 15 U.S.C. §§ 1681-1681x).

[28] *See* Data Broker Accountability and Transparency Act of 2014, S. 2025, 113th Cong. (2014), *available at* http://www.commerce.senate.gov/public/?a=Files.Serve&File_id=13d141a3-76b8-4191-810b-ebbfd5125759.

[29] *See* Julie Brill, Op-Ed., *Demanding Transparency from Data Brokers*, WASH POST, Aug. 15, 2013, *available at* http://articles.washingtonpost.com/2013-08-15/opinions/41412540_1_data-brokers-fair-credit-reporting-act-data-fuel; Julie Brill, Commissioner, Fed. Trade Comm'n, Keynote Address at 23rd Computers Freedom and Privacy Conference: Reclaim Your Name (June 26, 2013), *available at* http://www.ftc.gov/speeches/brill/130626computersfreedom.pdf.

Here's how it would work. Through creation of a consumer friendly one-stop on-line shop, Reclaim Your Name would empower the consumer to find out how data brokers are collecting and using her data; give her access to information that data brokers have amassed about her; allow her to opt-out if she learns a data broker is selling her information for marketing purposes; and provide her the opportunity to correct errors in information used for substantive decisions. In addition, data brokers that participate in Reclaim Your Name would provide more robust control tools for information involving health, finances and other sensitive issues.

5. Encourage global interoperability

As the children in rural India involved in Dr. Mitra's experiment can attest, appropriate technology and global data flows can provide immense benefits. As a result, interoperability among different national jurisdictions is critical. Our task, as policy makers, is to ensure that our different legal regimes facilitate rather than impede this beneficial interconnectedness. However, the story does not end there. Our collective task is to ensure that we also protect consumer privacy as data flow across borders.

As the OECD's Revised Privacy Guidelines highlight, the twin goals of interoperability and enhancing privacy protection can be mutually supportive.[30] The Guidelines encourage member countries not to restrict transborder flows of data where sufficient safeguards for privacy exist. The Guidelines encourage global interoperability not only in their explicit references to this issue, but also in the privacy principles themselves, which establish common ground on privacy issues across a wide range of jurisdictions.

The U.S.-EU Safe Harbor Framework and APEC's Cross-Border Privacy Rules System are two important mechanisms that both support interoperability and beneficial data transfers, and enhance privacy protections. As many of you know, I believe the Safe Harbor plays a critical role in enhancing the ability of my agency, the FTC, to protect the privacy of European citizens. We should support the continuation of these programs and others that both foster interconnectedness and enhance consumer privacy.

* * * *

Policy makers, academics, consumer advocates, and business leaders all have a role to play in enhancing consumer privacy protection in this age of big data, cross border data flows, and other rapid technological development. If we collectively work to implement the steps I've outlined, then we can create a global ecosystem that respects consumer privacy and engenders consumer trust, allowing big data to reach its full potential to thrive and benefit us all.

[30] *See* ORGANIZATION FOR ECONOMIC CO-OPERATION AND DEVELOPMENT, *Recommendation of the Council Concerning Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data* (2013), *available at* http://www.oecd.org/sti/ieconomy/2013-oecd-privacy-guidelines.pdf.