Commissioner Julie Brill
Keynote Address at the
University of Amsterdam Institute for Information Law and
University of California Berkeley Law School
Workshop on Online Tracking
Brussels, Belgium
February 11, 2013

Thank you, Nico, for that kind introduction, and thank you to the University of Amsterdam Institute for Information Law and the University of California Berkeley Law School for inviting me to speak to you today. It is a pleasure to be here to discuss privacy implications of consumer tracking, and to have the opportunity, once again, to continue a dialogue with my colleagues from Europe and the US.

Technology is transforming our lives. Its enormous benefits have become part of our daily routine. Tripadvisor plans our travel. Google Now keeps us on schedule. Birthdays are celebrated on Facebook. And our newborns' first pictures appear on Instagram.

But these now-familiar services are just the beginning of our connected future. Our cars are becoming computers with wheels,

wearable medical devices will be able to notify others when we are ill, and connected appliances might soon be able to tell us that we've made enough trips to the refrigerator for one night. These transformative online and mobile experiences collectively yield an enormous amount of data about us.

Technology used by others reaps even more data every minute we walk the street, park our cars, or enter a building. When we go outside, CCTV and security cameras capture our movements. Some retailers are using video surveillance, facial recognition, and cell phone signals to track customers' in-store movements.[1] And every time we go online or use a smartphone or credit card, our purchases and movements are tracked. 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 One estimate, already more than two years out of date, suggests that 1.8 trillion gigabytes of data were created in the year 2011 alone – that's the

[1] *See* Lisa Wirthman, *What Your Cellphone Is Telling Retailers About You*, FORBES EMCVOICE, Dec. 16, 2013, *available at* http://www.forbes.com/sites/emc/2013/12/16/what-your-cellphone-is-telling-retailers-about-you/.

equivalent of every U.S. citizen writing three tweets per minute for almost 27,000 years.[2] Ninety percent of the world's data, from the beginning of time until now, has been generated over the past two years,[3] and it is estimated that that total will double every two years from now on.[4]

Big data will have important, even transformative uses. No one questions some of the benefits big data analytics can bring. They include increased personalization for daily activities – helping companies determine which ads you see online, which articles a newspaper recommends to you, and which book to recommend you read next. But the potential benefits may also address important societal issues: keeping kids in high school;[5] conserving our natural resources by

[2] 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.

[3] Science News, *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.

[4] Steve Lohr, *The Age of Big Data*, N.Y. TIMES, Feb. 11, 2012, *available at* http://www.nytimes .com/2012/02/12/sunday-review/big-datas-impact-in-the-world.html?pagewanted=all&_r=0.

[5] 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.

making our use of electricity more efficient;[6] providing first responders in crisis situations with real-time information about the injured or those who lack power, water, or food;[7] and performing other miracles in the health care sector. Indeed, the opportunities big data analytics may provide in the field of medicine are staggering: prevention of infections in premature children,[8] access to mobile apps that distribute information to clinicians about bacteria types and resistance patterns in relevant communities,[9] and the development of preventative programs that anticipate a person's health status.[10]

(discussing efforts to reduce the high school drop-out rate using student record analysis in Mobile County, Alabama).

[6] *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).

[7] *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/#.

[8] 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*.

[9] *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/.

[10] *See id.*

While we are all eager to reap the potential benefits of big data, consumers, policy makers, and academics also see threats from these vast storehouses of data. 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.

This examination is becoming all the more urgent as phones, cars, and other everyday objects join the Internet of Things. Again, the potential benefits may be profound. Medical wearable devices—such as Google's contact lenses that help diabetics track glucose levels in their tears[11]—have the potential to affect millions of people suffering from a wide range of health conditions. But "smart" devices are about to become always-on sources of deeply personal information. This will be a big shift for consumers. Instead of having a handful of devices that mainly serve to connect them to the Internet, consumers may have many

[11] *See* Brian Fung, *Yes, Google Glass Users Look Weird. But Google's Smart Contact Lens Will Change All That*, WASH. POST, Jan. 17, 2014, *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/.

devices that they buy for one purpose – making coffee, storing food, driving to work – but that collect and use a vast amount of personal information about them. Whether it is a connected car, home appliance, or wearable device, the data that these connected devices generate could be higher in accuracy, quantity, and sensitivity and, if combined with other online and offline data, have the potential to create alarmingly personal consumer profiles.

Will consumers know that connected devices are capable of tracking them in new ways, especially when many of these devices have no user interface? How will these new sources of data flow into the huge constellation of personal data that already exists? Will companies that for decades have manufactured appliances and other "dumb" devices take the steps necessary to keep secure the vast amounts of personal information that their newly smart devices will generate?[12]

[12] *See* Julie Brill, Op-Ed., *From Regulators, Guidance and Enforcement (contribution to Room for Debate: Privacy, When Your Shoes Track Every Step)*, N.Y. TIMES, Sept. 8, 2013, *available at* http://www.nytimes.com/roomfordebate/2013/09/08/privacy-and-the-internet-of-things/regulators-must-guide-the-internet-of-things.

Similar questions arise in the ongoing discussion about online tracking. For several years now, regulators and industry standard-setting organizations, among others, have focused on cookie-enabled online tracking, and on providing consumers appropriate choices about such tracking.[13] But in recent months, we have seen industry turn its attention to developing other technologies to track consumers. Fingerprinting, which could uniquely identify a consumer's browser and obviate the need for cookies, would provide consumers with even less control.[14] As consumers turn increasingly to their smartphones and tablets, where cookies do not work, industry has deployed other mechanisms to track consumers.[15] How will these tracking technologies affect consumers' ability to provide consent? And how will consumers know the scope of

[13] *See generally* World Wide Web Consortium, Tracking Protection Working Group, http://www.w3.org/2011/tracking-protection/ (last visited Feb. 11, 2013). *See also* Directive 2009/136/EC of the European Parliament and of the Council of 25 November 2009 amending Directive 2002/22/EC on universal service and users' rights relating to electronic communications networks and services, Directive 2002/58/EC concerning the processing of personal data, and the protection of privacy in the electronic communications sector and Regulation (EC) No 2006/2004 on cooperation between national authorities responsible for the enforcement of consumer protection laws, 2009 O.J. (L 337) 11, 36, *available at* http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2009:337:0011:0036:EN:PDF.

[14] *See* Chris Jay Hoofnagle, Ashkan Soltani, Nathaniel Good, Dietrich J. Wambach, & Mika D. Ayenson, *Behavioral Advertising: The Offer You Cannot Refuse*, 6 HARV. L. & POL'Y REV. 274 (2012).

[15] *See* Erin Mershon, *Technology Outpacing Do Not Track Debate*, POLITICO PRO, Feb. 6, 2014.

information being collected, whether it is being shared with third parties, to whom, and for what purpose?

These questions echo the ones that have long surrounded the vast amount of data collection and profiling performed by ad networks, data brokers, and other entities that consumers generally know nothing about because they are not consumer facing. In some instances, these entities track consumers' online behavior. In other instances, these entities merge vast amounts of online and offline information about individuals, turn this information into profiles, and market this information for purposes that may fall outside of the scope of our current regulatory regime.

As we further examine the privacy implications of tracking and 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 sexual orientation, health conditions, financial condition, and race.

Let's look at a well-known, even 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 prediction" score.[16] Target was able to calculate, not only *whether* a consumer was pregnant, but also *when* her baby was due.[17] It used the information to win the expectant mom's loyalty by offering coupons tailored to her stage of pregnancy.[18]

To be clear, I don't have any information indicating that Target sold its pregnancy predictor score or lists of pregnant customers to third

---

[16] *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/.

[17] *See id.*

[18] *See id.*

parties, or that doing so would have violated the law. Yet we can easily imagine a company that could develop algorithms that will predict other health conditions – diabetes, cancer, mental illness – based on store purchases and other seemingly innocuous activities, and sell that information to marketers and others.

And actually, you don't have to imagine it. A recent U.S. Government Accountability Office (GAO) report states that at least one data broker includes in its profiles about consumers information about 28 or more specific diseases, including cancer, diabetes, clinical depression, and prostate problems.[19] According to a U.S. Senate staff report released last month, another data broker 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.[20] And we recently read reports about another

[19] *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).

[20] *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

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.[21] All of this is happening outside of HIPAA – outside any US regulatory scheme to protect this information.

Another troubling practice that we need to address is the creation and sale of profiles to identify financially vulnerable consumers. A number of the consumer lists that data brokers sell carry such titles as "Rural and Barely Making It," "Ethnic Second-City Strugglers," "Tough Start: Young Single Parents," and "Credit Crunched: City Families."[22] The Senate staff report said the names and descriptions of such products likely appeal to purveyors of payday loans and other financially risky

---

documentary submission from Equifax and listing health care-related data elements that Equifax maintains) [hereinafter "DATA BROKER REPORT"].

[21] *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.

[22] *See* STAFF OF S. COMM. ON COMMERCE, SCIENCE, AND TRANSP., DATA BROKER REPORT, *supra* note 20, at 24.

products to help them identify vulnerable consumers most likely to need quick cash.[23]

Some argue that if data brokers aren't employing predictions about health conditions or other sensitive personal traits for legally forbidden uses, then what is the harm? In fact, these advocates will say that predictive information about health conditions could help consumers reduce their risk of disease or make them aware of new opportunities for credit, clinical trials, and more benefits that outweigh any breach of privacy. But this view fails to account for the growing level of concern that consumers have about their most sensitive information being collected and stored in individual profiles and used for purposes that consumers do not know about and therefore cannot control.

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

[23] *See id.*

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 NSA to acknowledge 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 several years, there is a further benefit: Americans 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, use, package, and 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 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,"[24] 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."[25]

During our ongoing discussion about NSA surveillance, national security, and privacy, leaders within the business community have joined the President in recognizing that rebuilding the trust of individuals is essential to the success of governmental and industry

[24] *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.

[25] *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/*.

programs and services built on big data analytics.[26] They urge adoption of enhanced privacy protections as a key part of strengthening this 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 society and individuals may reap from appropriate and careful use of data analytics – will not be reached until we address some of these key consumer privacy concerns stemming from the creation, collection and use of sensitive consumer data and profiles.

[26] 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 Sorell, "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").

Here are the steps I believe must 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.[27] The FTC has developed best practices 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;

[27] In an analysis just 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.

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.[28]

Robust deidentification efforts along these lines will solve some of the problem. But such robust deidentification 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 – or as a recent trade association's report refers to it – "individual-level consumer data".

2. Create Institutional Ethical Monitoring

Another solution offered to the challenges big data presents to privacy is the creation of entities that monitor the ethical use of data.

[28] *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 [hereinafter "FTC PRIVACY REPORT"].

One proposal calls for the creation of "Consumer Subject Review Boards" to determine whether particular projects using consumer data are both legal and ethical.[29] Another proposal calls for individual companies to install the "algorithmist" – a licensed professional with ethical responsibilities for an organization's appropriate handling of consumer data.[30] But the Consumer Subject Review Boards and the algorithmist 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 help. As some of you have heard me say before, we have pretty good laws in the US governing commercial

[29] *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.

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

privacy, and we have excellent enforcement. The FTC—the leading privacy regulator in the United States—has built a robust data protection and privacy enforcement program that focuses on both traditional offline products and services,[31] as well as on the evolving digital and mobile marketplace.[32] The FTC uses its authority to stop unfair or deceptive practices that violate consumers' privacy or place consumers' data at risk.[33] We also enforce laws that protect consumers' financial[34] and health[35] information, information about children,[36] and information used

[31] *See, e.g., U.S. v. Check Servs., Inc.*, No. 1:13-cv-01247 (D.D.C. Aug. 15, 2013), *available at* http://www.ftc.gov/sites/default/files/documents/cases/2013/08/130815certegyorder.pdf; *U.S. v. PLS Fin. Servs., Inc.*, No. 1:12-cv-8334 (N.D. Ill. Oct. 26, 2012) (stipulated final judgment and order), *available at* http://www.ftc.gov/sites/default/files/documents/cases/2012/11/121107plspaydaystip.pdf; In the Matter of Rite Aid Corp., FTC File No. 072 3121 (Nov. 10, 2010) (decision and order). *available at* http://www.ftc.gov/sites/default/files/documents/cases/2010/11/101122riteaiddo.pdf.

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

[33] 15 U.S.C. §45(a).

[34] 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.).

[35] 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.

[36] 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).

to make decisions about credit, insurance, employment, and housing.[37] We engage in rigorous data security enforcement, as was clear when we announced our 50th data security enforcement action earlier this month. And, notably, the FTC vigorously enforces the U.S.-EU Safe Harbor Framework, as demonstrated by our recent actions against thirteen companies with false membership claims.[38] I believe that Safe Harbor is an appropriate data transfer mechanism that gives the FTC an effective tool to protect the privacy of EU citizens.[39]

Yet I believe we need to improve our commercial privacy laws in the US. When I talk about these issues in Washington, I call on Congress to enact legislation that would require data brokers to provide

---

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

[38] *See* Press Release, FTC Settles With Twelve Companies Falsely Claiming to Comply With International Safe Harbor Privacy Framework (Jan. 21, 2014), http://www.ftc.gov/news-events/press-releases/2014/01/ftc-settles-twelve-companies-falsely-claiming-comply; Press Release, FTC Settles With Children's Gaming Company for Falsely Claiming to Comply With International Safe Harbor Privacy Framework (Feb. 11, 2014), http://www.ftc.gov/news-events/press-releases/2014/02/ftc-settles-childrens-gaming-company-falsely-claiming-comply.

[39] *See* Julie Brill, Commissioner, Fed Trade Comm'n, At the Crossroads, IAPP Europe Data Protection Congress Keynote Speech (Dec. 11, 2013), *available at* http://www.ftc.gov/sites/default/files/documents/public_statements/crossroads-keynote-address-iapp-europe-data-protection-congress/131211iappkeynote.pdf.

notice, access, and correction rights to consumers scaled to the sensitivity and use of the data at issue. Such a law should require data brokers to give consumers the ability to access their information and correct it when it is used for eligibility determinations, and the ability to opt-out of information used for marketing. In addition, baseline privacy legislation for the commercial arena would close the gaps in consumer privacy protections and help level the playing field among businesses. And I think it is increasingly clear that the United States needs data security legislation.

4. Provide Consumers With Tools to Make Choices

But we need action now to address consumers' loss of control over their most private and sensitive information, even before legislation is enacted. To this end, I started a comprehensive initiative – "Reclaim Your Name" – that would give consumers the knowledge and the

technological tools to reassert some control over their personal data.[40] Put simply, consumers should have more control over decisions like how much to share, with whom, and for what purpose – to reclaim their names.

Here's how it would work. Through creation of consumer friendly online services, Reclaim Your Name would empower the consumer to find out how 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.

Improving the handling of sensitive data is another part of Reclaim Your Name. Data brokers that participate in Reclaim Your Name would

[40] *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.

agree to tailor their data handling and notice and choice tools to the sensitivity of the information at issue. As the data they handle or create becomes more sensitive – relating to health conditions, sexual orientation, and financial condition, for example – data brokers would provide greater transparency and more robust notice and choice to consumers.

The user interface is also critical. It should be user-friendly, and industry should provide a one-stop shop so consumers can learn about the tools all data brokers provide, and the choices consumers can make about the use of their data.

And it is critical that we move beyond single-company portals. Because data brokers are exchanging information with one another, consumers need an industry-wide solution that will allow them access across a broader swath of the ecosystem.

The Reclaim Your Name initiative meshes nicely with the ongoing work on a universal, simple, persistent, and effective Do Not Track mechanism that allows a consumer to stop companies from mining cyberspace for information about her for marketing purposes. First in 2010[41] and then again in 2012,[42] the FTC called for a system that would allow consumers to make choices about tracking that would travel with them wherever they went in cyberspace; that would apply across the ecosystem to all types of tracking; that would be easy to find and use; and that would let consumers stop both targeted ads and, importantly, the collection of their personal information as they browsed online or used their mobile devices.

Since 2010, there has been progress toward our vision of Do Not Track. Major browsers permit users to send instructions not to track

---

[41] *See* FED. TRADE COMM'N, PROTECTING CONSUMER PRIVACY IN AN ERA OF RAPID CHANGE: A PROPOSED FRAMEWORK FOR BUSINESSES AND POLICYMAKERS, PRELIMINARY FTC STAFF REPORT 66-69 (2010), *available at* http://www.ftc.gov/sites/default/files/documents/reports/federal-trade-commission-bureau-consumer-protection-preliminary-ftc-staff-report-protecting-consumer/101201privacyreport.pdf.

[42] *See* FED. TRADE COMM'N, FTC PRIVACY REPORT, *supra* note 28, at 53.

across websites. The Digital Advertising Alliance has deployed an icon-based opt out system – the About Ads Program – and has promised to work collaboratively with browsers so that consumers' choices will be persistent and honored no matter how they are initially exercised.[43] And an international standards-setting organization – the W3C – has convened a working group to create a universal Do Not Track standard through a consensus-based process with representatives from across the spectrum of stakeholders. The State of California's recently enacted law requiring websites that collect personally identifiable information to disclose both how they respond to Do Not Track signals and whether personally identifiable information about a consumer's online activities can be collected when the consumer uses the website [44] acts as an additional incentive for these various initiatives to cross the finish line. And here in the EU, the legislative proposal to reform the EU data protection framework reinforces the principle that companies should

[43] *See* Digital Advertising Alliance, White House, DOC and FTC Commend DAA's Self-Regulatory Program to Protect Consumer Online Privacy, DAA Announces Plans to Expand Program Consumer Choice Mechanisms, Feb. 23, 2012, https://www.aboutads.info/resource/download/DAA%20White%20House%20Event.pdf.

[44] *See* Cal. Bus. & Prof. Code § 22575(b)(5)-(6).

obtain consumers' consent before collecting and sharing consumer data.[45] I urge all of the stakeholders to forge ahead with their work and reach consensus to implement an effective, universal and comprehensive Do Not Track system.

If consensus is reached, Do Not Track would allow consumers to choose when their online data can be monitored for marketing purposes. Reclaim Your Name would give consumers the power to access online and offline data already collected, exercise some choice over how their data will be used in the commercial sphere, and correct any errors in information being used by those making decisions seriously impacting the consumers' lives.

Policy makers, academics, consumer advocates, and industry representatives are all encouraging industry to take more aggressive

[45] *See Commission Proposal for a Directive of the European Parliament and of the Council on the Protection of Individuals with regard to the Processing of Personal Data and on the Free Movement of such Data (General Data Protection Regulation)*, COM (2012) 11 amended (Oct. 21, 2013), *available at* http://www.europarl.europa.eu/meetdocs/2009_2014/documents/libe/dv/comp_am_art_01-29/comp_am_art_01-29en.pdf, http://www.europarl.europa.eu/meetdocs/2009_2014/documents/libe/dv/comp_am_art_30-91/comp_am_art_30-91en.pdf (listing the European Parliament Committee on Civil Liberties, Justice, and Home Affairs's latest amendments to Articles 1-91).

action to protect consumer privacy. By implementing the steps I've outlined, industry (and policy makers) can help create an ecosystem that respects consumer privacy and engenders consumer trust, allowing big data to reach its full potential to thrive and benefit us all.