Commissioner Julie Brill
"Big Data and Consumer Privacy:
Identifying Challenges, Finding Solutions"
Address at the Woodrow Wilson School of
Public and International Affairs
Princeton, University
February 20, 2014

Thank you, Ed, for that kind introduction and for inviting me to speak today. It is always a pleasure to come home to Princeton, and today is no exception. Princeton, and in particular the Woodrow Wilson School, cultivates leaders of all types and in many fields, including those that have helped fuel our global technological revolution. As a lifelong consumer protection advocate, I have spent a lot of time focusing on the privacy implications of emerging technologies. Today, I would like to focus on one of the fastest growing and most promising areas in our technological revolution – big data analytics – and its effect on consumer privacy.

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 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.

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 use 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 One estimate, already more than two years out of date, suggests that 1.8 trillion gigabytes of data were created in the year 2011 alone – that's the equivalent of every U.S. citizen writing three tweets per minute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,

[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/.

[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.

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]

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 aims for loftier goals. It promises to bring us more profound benefits by addressing important societal issues like keeping kids in high school;[5] conserving our natural resources by 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] mobile apps that distribute information to clinicians about bacteria types and resistance patterns in relevant communities,[9] and the development of preventive programs that anticipate a person's health status.[10]

We are all eager to reap the potential benefits of big data. Yet 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.

[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. (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/ (discussing the use of big data to predict individuals' health status and guide preventative health programs).

[10] *See id.*

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 – a smartphone, tablet and laptop – that mainly serve to connect consumers to the Internet, consumers may have many 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 – could 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? 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? And how will the new data from all of these connected devices flow into the huge constellation of personal data that already exists about each of us?[12]

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 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, 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

[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/.

[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.

predictor score."[13] Target was able to calculate, not only *whether* a consumer was pregnant, but also *when* her baby was due.[14] It used the information to win the expectant mom's loyalty by offering coupons tailored to her stage of pregnancy.[15]

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 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. The U.S. Government Accountability Office (GAO) reports that one data broker includes in its consumer profiles information about 28 or more specific diseases, including cancer, diabetes, clinical depression, and prostate problems.[16] 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.[17] 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.[18] All of this creation, analysis and use of consumers' health information is happening outside of HIPAA – outside the US regulatory regime designed to protect health 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

[13] *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/.

[14] *See id.*

[15] *See id.*

[16] *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).

[17] *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"].

[18] *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.

Start: Young Single Parents," and "Credit Crunched: City Families."[19] I am concerned that the names and descriptions of such products likely appeal to purveyors of payday loans and other financially risky products to help them identify vulnerable consumers most likely to need quick cash.[20]

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? These advocates will say that predicting consumers' health conditions could help them reduce their risk of disease or make them aware of new opportunities for clinical trials, and predicting their financial situation could help them find new opportunities for credit – 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 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 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, 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 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,"[21] and when he called

[19] *See* STAFF OF S. COMM. ON COMMERCE, SCIENCE, AND TRANSP., DATA BROKER REPORT, *supra* note 17, at 24.

[20] *See id.*

[21] *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.

for a "national conversation…about…the general problem of … big data sets, because this is not going to be restricted to government entities."[22]

During our ongoing discussion about government 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 all programs and services – both governmental and commercial – built on big data analytics.[23] 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 four 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. And, importantly, each of you will play a critical role in solving these problems.

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.[24] My agency, the Federal Trade Commission, has developed best practices around deidentification that strike an appropriate balance and include both robust

[22] *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/*.

[23] 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").

[24] 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.

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.[25]

Robust deidentification efforts along these lines will solve some of the problem. And the creation of more effective tools to deidentify data – something that I am confident that many in this room could develop – would also help. 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.[26]

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. One proposal calls for the creation of "Consumer Subject Review Boards" to determine whether particular projects using consumer data are both legal and ethical.[27] 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.[28] And I know that Ed Felten's students in Princeton computer science and engineering programs are encouraged to examine the ethical implications of designing algorithms, computer programs, and other innovative projects. More engineering and computer science schools should follow Professor Felten's lead. Yet ethically trained computer scientists, algorithmists, and Consumer Subject Review Boards 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.

[25] *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.

[26] *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.

[27] *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.

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

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.[29] The FTC uses its authority to stop unfair or deceptive practices that violate consumers' privacy or place consumers' data at risk.[30] We also enforce laws that protect consumers' financial[31] and health[32] information, information about children,[33] and information used to make decisions about credit, insurance, employment, and housing.[34] We engage in rigorous data security enforcement, as was clear when we announced our 50th data security enforcement action earlier this month.

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. First, I call on Congress to enact 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. 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. Thankfully, Senate Commerce Committee Chairman Rockefeller and Senator Markey of Massachusetts have just introduced such a bill.[35] Second, I believe adoption of baseline privacy legislation for the commercial arena would close the gaps in consumer privacy protections and help level the playing field among businesses. And third, I think it is increasingly clear that the United States needs data security legislation. For those of you who are

[29] *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).

[30] 15 U.S.C. §45(a).

[31] 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.).

[32] 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.

[33] 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).

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

[35] *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.

interested in these policy issues, we need your fresh perspective on how this era of rapid technological change has challenged our privacy framework here in the US, and we need your intellect and tenacity to help develop robust solutions.

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. To this end, I have 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.[36] 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 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.

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

In sum, 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 affecting consumers' lives. You could help develop Reclaim Your Name or similar solutions to bring more transparency to the data broker industry, and help enhance consumer privacy.

* * * *

[36] *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.

Policy makers, academics, consumer advocates, and business leaders are all encouraging industry to take more aggressive action to protect consumer privacy. Computer scientists, engineers, programmers, and technologists also have a valuable set of skills that should be put to the task of solving some of these critical privacy issues. If we collectively work to implement the steps I've outlined, and other steps that you may develop, then we can 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.