Reclaim Your Name
23rd Computers Freedom and Privacy Conference
Keynote Address by
Commissioner Julie Brill
Federal Trade Commission
Washington, DC
June 26, 2013

Thank you for that generous introduction and for allowing me the opportunity to speak to you. Today I'd like to address big data and the challenges it presents for consumers, for markets, and for agencies like the FTC tasked with safeguarding both. The topic is timely. This month, Edward Snowden, a former employee of a national security contractor, gave the world a crash course in just how much privacy we can expect if we participate at all in an increasingly online and mobile marketplace. He leaked details of some of the National Security Administration's data collection efforts, one program that collects telephone metadata from US telephone companies and another that monitors international Internet and email traffic.

We don't have to pass judgment on the NSA or Snowden to acknowledge the 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.

Many consumers have been loath to examine too closely the price we pay, in terms of forfeiting control of our personal data, for all the convenience, communication, and fun of a free-ranging and mostly free cyberspace. We are vaguely aware that cookies attach to us wherever we go, tracking our every click and view. We tell Trip Advisor our travel plans, open our calendars to Google Now, and post our birthdays on Facebook. We broadcast pictures of our newborns on Instagram; ask questions about intimate medical conditions on WebMD; and inform diet sites what we ate that day and how long we spent at the gym. Google Maps, Twitter and Four Square know where we are. Uber, Capital BikeShare, and Metro's trip planner know where we're going and how we plan to get there.

We spew data every minute we walk the street, park our cars, or enter a building – the ubiquitous CCTV and security cameras blinking prettily in the background – every time we go online, use a mobile device, or hand a credit card to a merchant who is online or on mobile. We spend most of our days, and a good deal of our nights, surfing the web, tapping at apps, or powering on our smart phones, constantly adding to the already bursting veins from which data miners are pulling pure gold. That's where the "big" in "big data" comes from.

We send our digital information out into cyberspace and get back access to the magic of our wired lives. We sense this, but it took Snowden to make concrete what exactly the exchange means – that firms or governments or individuals, without our knowledge or consent, and often in surprising ways, may amass private information about us to use in a manner we don't expect or understand and to which we have not explicitly agreed.

It is disconcerting to face how much of our privacy we have already forfeited. 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 last week when he called for a "national conversation…about the general problem of these big data sets because this is not going to be restricted to government entities."

I'd like to pose two questions that are key to getting this conversation going, and then spend some time today trying to answer them. First, what are the major challenges to privacy posed by big data, particularly in its use in the commercial arena? And second, what steps can we take to meet these challenges?

But before I start, I want to make clear that big data is not synonymous with the evil empire. Most of us, myself included, rely on and enjoy our phones, apps, emails, and other programs that collect, store, and analyze large stocks of raw data. In their book, *Big Data*[1], Victor Mayer-Schonberger and Ken Cukier cite numerous examples of how big data benefits us every day: spam filters adapt as junk email changes; dating sites pair couples based on attributes that correlate to previous successful matches; cars brake before we sense danger; online bookstores tell us what we will want to read next.

And these benefit go beyond making sure we don't receive announcements of bogus lottery winnings or suffer through too many awkward blind dates – though I have single friends who tell me the latter innovation is Nobel Prize quality stuff. Big data is already revolutionizing health care. Mayer-Schonberger and Cukier write of Google, in 2009, analyzing the correlation between relevant user searches, such as "medicines for cough and cold," and reported flu outbreaks from past years, to predict where – down to the region and state – H1N1 would strike. Another more recent example is the research project dubbed "Artemis" underway at Toronto's Hospital for Sick Children. Doctors there are collecting and analyzing second-by-second vital statistics for premature newborns. They hope the resulting big database will allow clinicians to spot the onset of infection – a serious threat to these infants – in time to treat it effectively or ward it off altogether.

The financial world has long employed big data. Actuaries were using demographics and other trends to set life and auto insurance rates long before insurance salesman Fred MacMurray tried to help his paramour Barbara Stanwyck beat the number crunchers to get a big payout in the 1944 film *Double Indemnity*. By the 1960s, with the

[1] VIKTOR MAYER-SCHONBERGER & KENNETH CUKIER, BIG DATA: A REVOLUTION THAT WILL TRANSFORM HOW WE LIVE, WORK, AND THINK, 11 (2013) (hereinafter Big Data).

advent of modern credit reporting agencies and their files on millions of Americans, consumers could access credit without knowing their bankers, thus greasing the wheels of the growing economy. But with the credit reporting agencies' large databases came errors and unease about the amount of information – and hence power – these agencies held, due to their new-found ability to draw inferences and correlations that were not possible a decade earlier. As a result, in 1970, Congress passed the Fair Credit Reporting Act,[2] which contains rules about how credit reporting agencies and their customers can use the information and inferences drawn from these large databases.

Fast forward to today. We are awash in data. Estimates are that 1.8 trillion gigabytes of data were created in the year 2011 alone – that's the equivalent of every U.S. citizen writing 3 tweets per minute for almost 27,000 years.[3] Ninety percent of the world's data, from the beginning of time until now, has been generated over the past two years,[4] and it is estimated that that total will double every two years from now on.[5] As the costs of storing data plummet and massive computing power becomes widely available, crunching large data sets is no longer the sole purview of gigantic companies or research labs. As Schonberger-Mayer and Cukier write, big data has become democratized.

First Challenge: the Fair Credit Reporting Act

This astounding spread of big data gives birth to its first big challenge: how to educate the growing and highly decentralized community of big data purveyors about the rules already in place governing the ways certain kinds of data can be used. For instance, under the Fair Credit Reporting Act, or "FCRA," entities collecting information across multiple sources and providing it to those making employment, credit, insurance and housing decisions must do so in a manner that ensures the information is as accurate as possible and used for appropriate purposes.

The Federal Trade Commission has warned marketers of mobile background and criminal screening apps that their products and services may come under the FCRA, requiring them to give consumers notice, access, and correction rights.[6] We've also

---

[2] Fair Credit Reporting Act, 15 U.S.C. § 1681 (1970).

[3] 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.

[4] *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.

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

[6] *See* Press Release, FTC Warns Marketers That Mobile Apps May Violate Fair Credit Reporting Act (Feb. 7, 2012), *available at* http://www.ftc.gov/opa/2012/02/mobileapps .shtm. The FTC has issued similar warning letters to app developers and data brokers that appeared to be selling consumer information for use in tenant screening, and in making insurance and employment decisions and firm offers of credit: *See* Press

entered into consent decrees that allow us to monitor the activities of other apps and online services that have similarly wandered into FCRA territory.[7] But while we are working hard to educate online service providers and app developers about the rules surrounding collecting and using information for employment, credit, housing, and insurance decisions, it is difficult to reach all of those who may be – perhaps unwittingly – engaged in activities that fall into this category.

Further, there are those who are collecting and using information in ways that fall right on —or just beyond —the boundaries of FCRA and other laws. Take for example the new-fangled lending institutions that forgo traditional credit reports in favor of their own big-data-driven analyses culled from social networks and other online sources.[8] Or eBureau, which prepares rankings of potential customers that look like credit scores on steroids. The New York Times describes this company as analyzing disparate data points, from "occupation, salary and home value to spending on luxury goods or pet food, … with algorithms that their creators say accurately predict spending."[9] These "e-scores" are marketed to businesses, which use them to decide to whom they will offer their goods and services and on what terms. It can be argued that e-scores don't yet fall under FCRA because they are used for marketing and not for determinations on ultimate eligibility. But what happens if lenders and other financial service providers do away with their phone banks and storefronts and market their loans and other financial products largely or entirely online? Then, the only offers consumers will see may be those tailored based on their e-scores. Without FCRA protections, a consumer would not know if her e-score led to a higher loan rate or insurance premium, nor would she be able to access and correct any erroneous information about her.

Another class of decisions increasingly based on big data – what the FTC has called "eligibility" determinations – can also – if founded on inaccurate information – do real harm to consumers.[10] These include determinations about whether a consumer is too risky to do business with, engaged in fraud, or ineligible to enroll in certain clubs, dating

---

Releases, e.g., FTC Warns Data Broker Operations of Possible Privacy Violations (May 7, 2013), *available at* http://www.ftc.gov/opa/2013/05/databroker.shtm, *and* FTC Warns Data Brokers That Provide Tenant Rental Histories They May Be Subject to Fair Credit Reporting Act (Apr. 3, 2013), *available at* http://www.ftc.gov/opa/2013/04/tenant.shtm.

[7] *See* Press Release, Marketers of Criminal Background Screening Reports To Settle FTC Charges They Violated Fair Credit Reporting Act (Jan. 10, 2013), *available at* http://www.ftc.gov/opa /2013/01 /filiquarian.shtm.

[8] Evelyn M. Rusli, *Bad Credit? Start Tweeting*, WALL ST. J., Apr. 1, 2013, *available at* *http://online.wsj.com/article/SB10001424127887324883604578396852612756398.html*.

[9] Natasha Singer, *Secret E-Scores Chart Consumers' Buying Power*, N.Y. TIMES, Aug. 18, 2012, *available at* *http://www.nytimes.com/2012/08/19/business/electronic-scores-rank-consumers-by-potential-value.html?pagewanted=all*.

[10] FED. TRADE COMM'N, Protecting Consumer Privacy in an Era of Rapid Change: Recommendations for Businesses and Policymakers (Mar. 26, 2012) (hereinafter 2012 Privacy Report) at 68 –70, *available at* http://www.ftc.gov/os/2012/03/12032 6privacyreport.pdf.

services, schools, or other programs. Though any of these decisions could deeply affect consumers, the data used to make them may not fall within the confines of the FCRA.

The FCRA is a law that establishes the fair and prudent use of certain types of consumer data, and it is a law that is both relevant and worth preserving. But our big data world strains the seams of the FCRA. Our challenge is to figure out how FCRA's principles can coexist with new ways of collecting and using information – how consumers can maintain notice, access, and correction rights on all the dossiers – not just credit reports – that inform important decisions on eligibility as well as offers in areas such as housing, employment, finances, and insurance.

Second Challenge: Transparency

The second big challenge to big data is transparency. Consumers don't know much about either the more traditional credit reporting agencies and data brokers or the newer entrants into the big data space. In fact, most consumers have no idea who is engaged in big data predictive analysis.

To their credit, some data brokers allow consumers to access some of the information in their dossiers, approve their use for marketing purposes, and correct the information for eligibility determinations.[11] In the past, however, even well-educated consumers have had difficulty obtaining meaningful information about what the data brokers know about them.[12] Just yesterday, "the big daddy of all data brokers", Acxiom, announced that it plans to open its dossiers so that consumers can see the information the company holds about them.[13] This is a welcome step. But since most consumers have no way of knowing who these data brokers are, let alone finding the tools the companies provide, the reality is that current access and correction rights provide only the illusion of transparency.

Third Challenge: Notice and Choice

A third challenge involves those aspects of big data to which the FCRA is irrelevant – circumstances in which data is collected and used for determinations unrelated to credit, employment, housing, and insurance, or other eligibility decisions. We need to consider these cases within the frameworks of the Federal Trade Commission

---

[11] *See*, e.g., AXCIOM, *available at* http://www.acxiom.com/site-assets/privacy-acxiom-marketing-products/ (last visited June 24, 2013); EPSILON, *available at* http://www .epsilon.com/consumer-info/consumer-guide-direct-marketing (last visited June 24, 2013); *and* EBUREAU, *available at* http://www.ebureau.com/privacy-center (last visited June 24, 2013).

[12] Natasha Singer, *Consumer Data, but Not for Consumers*, N.Y. TIMES, Aug. 18, 2012, *available at* http://www.nytimes.com/2012/07/22/business/acxiom-consumer-data-often-unavailable-to-consumers.html?pagewanted=all&_r=1& .

[13] Adam Tanner, *Finally You'll Get to See the Secret Consumer Dossier They Have On You*, FORBES, June 25, 2013, *available at* http://www.forbes.com/sites/adamtanner/2013/06/25/finally-youll-get-to-see-the-secret-consumer-dossier-they-have-on-you/ .

Act, the OECD's Fair Information Privacy Principles,[14] and the FTC's 2012 Privacy Report,[15] for it is within those contexts we can see how big data is testing established privacy principles such as notice and choice.

One comparison highlights the difficulties of providing notice and consent in the context of big data – that of Artemis, the Toronto research project on infections in premature newborns, and the well-known, even infamous, example of the department store Target's big-data-driven campaign to identify pregnant customers. Over a year ago, the New York Times reported on Target's efforts to develop, through analysis of consumers' purchases at its stores, a "pregnancy prediction" score.[16] Target was able to calculate, not only whether a consumer was pregnant, but also when her baby was due. It used the information to win the consumer's loyalty by offering coupons tailored to her stage of pregnancy.

Obviously, Artemis and Target use big data for different ends: saving the lives of premature infants versus selling more maternity clothes and bassinettes. There's no value judgment in that statement: Medical researchers look to improve our health; department stores seek to sell us stuff. We all want infant mortality to decline, and we all need a place to go to buy inexpensive baby clothes and diapers. The important point here is that, because of the context of the different relationships at issue, Artemis's use of Big Data allows for meaningful notice and choice within an appropriate regulatory regime, whereas Target did not – could not – provide meaningful notice and choice about its pregnancy predictor score project.

Artemis and other quality research projects inform parents of the data they are collecting from the babies and receive consent to do so.[17] Indeed, collecting information about their premature infants in order to provide better care is a critical part of the context of the relationship between the parents and the hospital.

Target's research and where it lands within the context of the retailer's relationship with the consumer is quite different. Let's assume Target didn't use any health information in creating its pregnancy predictor score, but instead tracked buying

---

[14] Organization for Economic Cooperation and Development, Guidelines on the Protection of Privacy and Transborder Flow of Personal Data, (Sept. 23, 1980) *available at* http://www.oecd.org/internet/ieconomy/oecdguidelinesontheprotectionofprivacyandtransborderflowsofpersonaldata.htm.

[15] 2012 Privacy Report, *supra* note 10.

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

[17] In the United States, the Health Insurance Portability and Accountability Act of 1996 (HIPAA), 42 U.S.C. § 1320d-9, requires hospitals, doctors, health insurance companies and their business partners are required to follow strict guidelines on how they handle health information about patients and insureds. And Institutional Review Boards ensure that human research is conducted ethically, including by maintaining the privacy of research subjects. *See* Institutional Review Board Guide Book at Chapter 3, http://www.hhs.gov/ohrp/archive/irb/irb_guidebook.htm .

patterns such as the purchase of prenatal vitamins and lotions with the subsequent purchase of newborn-size diapers. Given the context of the consumer's retail relationship with the store, I believe it would be impossible for Target to ask the consumer in a meaningfully way to consent to participating in the market study. The whole point of Target's big data project – indeed the point of many such big data projects – is to take innocuous information – here purchases at a store – and create an algorithm that makes sensitive predictions – here, whether a customer is pregnant.

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. Yet we can easily imagine a company that could develop algorithms that will predict other health conditions – diabetes, cancer, mental illness – based on information about routine transactions – store purchases, web searches, and social media posts – and sells that information to marketers and others.

And actually, you don't have to imagine it; it is already happening. The Financial Times recently highlighted how some data brokers collect personal details so intimate it makes Target's efforts seem almost quaint. One firm, LeadsPlease.com, reportedly sells the names, mailing addresses, and medication lists of people with diseases like cancer or clinical depression. Another data broker, ALC Data, reportedly offers lists of consumers, their credit scores, and their specific ailments.[18]

Undoubtedly Target (and other companies in a similar position) provides some notice about how it collects and uses information to its *online* shoppers. But there is nothing in the context of a retail purchase that implies notice and consent – nothing that reasonably informs the consumer her data might be collected to make predictions about sensitive health conditions or seeks her consent to do so. And if the store were to try to make the notice and consent explicit? Imagine walking into Target and reading a sign on the wall or a disclosure on a receipt that says: "We will analyze your purchases to predict what health conditions you have so that we can provide you with discounts and coupons you may want." That clear statement would surprise – and alarm – most of us.

Big data advocates will point out that the FCRA delineates the inappropriate uses of sensitive data like health status. If data brokers aren't employing their health projections for one of these 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 control their symptoms, an end result that more than balances any breach of privacy.

The argument is compelling. But when health information flows outside the protected HIPAA environment, I worry about three things. First, as I mentioned before, how sensitive health information might be used to make decisions about eligibility that fall outside the contours of the FCRA, without notice or choice to the consumer. Second,

[18] Emily Steel, *Companies scramble for consumer data*, FINANCIAL TIMES, June 12, 2013, *available at* http://www.ft.com/intl/cms/s/0/f0b6edc0-d342-11e2-b3ff-00144feab7de.html#axzz2XEcog1Gh.

what will happen if this sensitive health information falls into the wrong hands through a data security breach – more on that in a minute. And third, what damage is done to our individual 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.

Fourth Challenge: Deidentification

The final big challenge of big data that I would like to discuss is one that I've been assured by many of its proponents I shouldn't strain too hard to solve – that of predictive analytics attaching its findings to individuals. Most data brokers and advertisers will tell you they are working with de-identified information, that is, data stripped of a name and address. And that would be great if we didn't live in a world where more people know us by our user names than our given ones. Our online tracks are tied to a specific smartphone or laptop through UDIDs, IP addresses, "fingerprinting" and other means. Given how closely our smartphones and laptops are associated with each of us, information linked to specific devices is, for all intents and purposes, linked to individuals.

Furthermore, every day we hear how easy it is to reattach identity to data that has been supposedly scrubbed. 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.[19] 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.[20]

Target was most certainly linking its pregnancy forecasts with individuals' names, street addresses, and maybe phone numbers, email and IP addresses. How else could the retailer deliver the targeted coupon offers? And we know nothing about how long Target planned to hold onto this health information, and in what form it would be held.

We are all very familiar with the harms that can occur when there is a data breach. The risk of those injuries is multiplied ten-fold by big data's need to collect and store vast amounts of linkable data. The very way big data works – churning through personal details collected and saved without a specific purpose or expiration date – flies in the face of data minimization, one of the main fair information principles embedded in "privacy by design". Reducing the real damage data breaches can cause is one reason the FTC is urging big data users to commit to a robust program to de-identify their information.

---

[19] Yves-Alexandre de Montjoye, et. al., *Unique in the Crowd: The privacy bounds of human mobility*, 3 SCI REP. 1376 (2013).

[20] ALESSANDRO ACQUISTI, et. al., HEINZ COLLEGE & CYLAB CARNEGIE MELLON UNIVERSITY, FACES OF FACEBOOK: PRIVACY IN THE AGE OF AUGMENTED REALITY, (draft version) (2011), *available at* http://www.heinz.cmu.edu/~acquisti/face-recognition-study-FAQ/acquisti-faces-BLACKHAT-draft.pdf.

Clearly, simply deleting the name and address columns from big databases is not enough to keep anonymous the private information collected from consumers. The FTC has called on companies trafficking in big data to take both technological and behavioral steps to make sure the information they use in their advertising is truly and completely de-identified. They 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.[21]

How would this work in practice? Say Des Moines, Iowa wants to solve its terrible rush hour traffic congestion problems. City planners believe that the most useful information to help them tackle the problem is cellphone data, because cell phones are always on, and the data from them uniquely depicts traffic patterns and bottlenecks. Of course, Verizon and Sprint could not just hand over their customer's cell phone data, because – in the FTC's view – geolocation information linked to an individual is classic sensitive personal data. But the carriers could, as best as possible, scrub the data of sensitive personal information, and then – before they hand it over or allow Des Moines to use it – require Des Moines to sign a contract that specifically prohibits any effort to re-identify the data in any way, or to provide it to other parties.

Robust deidentification efforts along these lines will solve some of the problem. But because much of big data is created through predictive analysis, and because much of the analytics are for the purpose of gaining insights into specific individuals, chunks of big data will always be, by their very nature, identifiable or linkable to individuals.

Solutions to Notice, Choice and Transparency

So let's turn to some ways to solve the challenges big data poses to meaningful notice and choice as well as transparency. A part of the solution will be for companies to build more privacy protections into their products and services, what we at the FTC call "privacy by design". We have recommended that companies engage in cradle-to-grave review of consumer data as it flows through their servers, perform risk assessments, and minimize and deidentify data wherever possible.[22] Mayer-Schonberger and Cukier have helpfully called for the creation of "algorithmists" – licensed professionals with ethical responsibilities for an organization's appropriate handling of consumer data.[23] But the algorithmist will only thrive in an environment that thoroughly embraces "privacy by design," from the C-suite to the engineers to the programmers.

And unfortunately, even if the private sector embraces privacy by design and we license a cadre of algorithmists, we will not have met the fundamental challenge of big

[21] 2012 Privacy Report, s*upra* note 10, at 21.

[22] *Id* at 22.

[23] Big Data, s*upra* note 1, at 180 – 182.

data in the marketplace: that is, consumers' loss of control of their most private and sensitive information.

Changing the law would help. I support 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. For example, Congress 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.

But we can begin to address consumers' loss of control over their most private and sensitive information even before legislation is enacted. I would suggest we need a comprehensive initiative – one I am calling "Reclaim Your Name." Reclaim Your Name would give consumers the knowledge and the technological tools to reassert some control over their personal data – to be the ones to decide how much to share, with whom, and for what purpose – to reclaim their names.

Reclaim Your Name would empower the consumer to find out how brokers are collecting and using 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 – like credit, insurance, employment, and other benefits.

Over a year ago, I called on the data broker industry to develop a user-friendly, one-stop online shop to achieve these goals. Over the past several months, I have discussed the proposal with a few leaders in the data broker business, and they have expressed some interest in pursuing ideas to achieve greater transparency. I sincerely hope the entire industry will come to the table to help consumers reclaim their names.

In addition, 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 – the data brokers would provide greater transparency and more robust notice and choice to consumers.

The credit reporting industry has to do its part, too. There are simply too many errors in traditional credit reports.[24] The credit bureaus need to develop better tools to help consumers more easily obtain and understand their credit reports so they can correct them. I have asked major credit reporting agencies to improve and streamline consumers' ability to correct information across multiple credit reporting agencies.

[24] *See* Press Release, In FTC Study, Five Percent of Consumers Had Errors on Their Credit Reports That Could Result in Less Favorable Terms for Loans (Feb. 11, 2013), *available at* http://www.ftc.gov/opa/2013/02/creditreport.shtm. The report revealed that one in twenty US consumers (10 million people) had errors in their credit report that could result in less favorable terms for credit.

I will continue to work on the contours of Reclaim Your Name over the next several months. I look forward to discussing the elements of this initiative with industry, consumer groups, and other stakeholders.

The Reclaim Your Name initiative meshes nicely with the FTC's ongoing interest in 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,[25] and then again in 2012,[26] 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, not just the serving of targeted ads, but the collecting 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 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. 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. I urge the W3C stakeholders to forge ahead with their work and reach consensus.

If consensus is reached, Do Not Track would allow consumers to choose when their online data is 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 materially impacting consumers' lives. Together, these policies will restore consumers' rights to privacy that big data has not just challenged but has abrogated in too many instances.

One of our nation's greatest social and political thinkers – the late Abigail Van Buren of "Dear Abby" fame – often said "No one can take advantage of you without your permission." That is such a perfectly American thought that I am surprised Jefferson didn't include it in his list of the truths we hold to be self-evident. It speaks to American self-reliance and independence – to our individual rights set in stone in the Declaration of Independence and the Bill of Rights.

And perhaps therein lies the biggest challenge of big data: it is taking advantage of us without our permission. Often without consent or warning, and sometimes in

---

[25] Protecting Consumer Privacy in an Era of Rapid Change: A Proposed Framework for Businesses and Policymakers, A Preliminary FTC Staff Report (Dec. 1, 2010) at 63 – 68, *available at* http://www .ftc .gov/os/2010 /12/101201privacyreport.pdf.

[26] 2012 Privacy Report, s*upra* note 10, at 52 – 55.

completely surprising ways, big data analysts are tracking our every click and purchase, examining them to determine exactly who we are – establishing our name, good or otherwise – and retaining the information in dossiers that we know nothing about, much less consent to.

There is no reason that big data cannot coexist with an effective Do Not Track mechanism and with a system that empowers consumers to make real choices about how their private information will be used. The ability to claim your name – or in the case of big data, Reclaim Your Name – is as American as Mom and apple pie. I can't believe consumers will give that up easily, even for all the convenience, entertainment and wonder that cyberspace currently has on offer. And I want to believe that industries currently fueled by big data will join together to help consumers reclaim their names.