A Call to Arms: The Role of Technologists in Protecting Privacy in the Age of Big Data

Sloan Cyber Security Lecture by Commissioner Julie Brill
Polytechnic Institute of NYU
Brooklyn, NY
October 23, 2013

Thank you, Kathy, for that kind introduction, and thank you President Sreenivasan for your opening remarks. I am honored to be here, and I'd like to thank the Sloan Foundation and NYU-Poly for sponsoring and hosting a great event.

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. Our newborns' first pictures appear on Instagram. We discuss our medical conditions with WebMD. Google Maps, Twitter and Foursquare know where we are. And Uber, Citi Bike, and MTA's trip planner know where we're going and how we're going to get there. 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, ubiquitous CCTV and security cameras capture our movements. Our new cars will track us. 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. And that rich vein of data is exactly the gold that data miners want to extract.

The estimates of the data we collectively generate are staggering. One estimate, already two years out of date, suggests that 1.8 trillion gigabytes of data were created in the year 2011 alone – that's the equivalent of every U.S. citizen writing 3 tweets per minute for almost 27,000 years.[1] Ninety percent of the world's data, from the beginning of time until now, has been generated over the past two years,[2] and it is estimated that that total will double every two years from now on.[3]

Some argue that this abundant data resource has become the "new oil". Businesses are eager to drill to unlock the mysteries of disease, unblock our traffic jams, and solve industry's version of Freud's age-old question: what do consumers really want?

---

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

[2] 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.

[3] 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.

Big data will have important, even transformative uses. But consumers, policy makers, and academics also see threats from these vast storehouses of data. This summer's revelations about the National Security Agency's vast data collection programs sound the alarm about the threat to privacy in a world where all one does is known and apparently is subject to government inspection. 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. We do not need to pass judgment on the NSA's program to begin an overdue debate on how to balance national security against citizens' privacy rights. But I would hope that the debate does not stop there. We need to have a similar debate in the commercial sphere as well, and the time to have it is now.

The debate about big data brings the issues in the commercial sphere into sharp focus. No one questions the benefits big data analytics can bring, from the utterly mundane – helping companies determine which ads you see online, which articles a newspaper recommends to you, and which book to recommend you read next – to the utterly transformative – keeping kids in high school,[4] preventing infections in premature children,[5] and conserving our natural resources by making our use of electricity more efficient.[6]

To reap these rewards, we're told, we need to scrap many of the basic privacy principles.[7] No more should companies worry about over-collection; no more should companies delete data. Data is the grist for their big analytic mill, and the more data the better. Impose "use restrictions" instead.[8] Consent? Especially for secondary uses? Out the window![9] Choice is inefficient and ineffective. And in any event, how can companies give consumers notice and choice about unknown, unanticipated uses of personal data, to be discovered later through Big Analytics?[10]

Today I'd like to answer these questions by presenting a different paradigm, a better paradigm. We can unlock the potential of big data and enjoy its benefits. But we can do so and

---

[4] 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).

[5] Brian Proffitt, Big data analytics may detect infections before clinicians, ITWORLD (April 12, 2012), *available at* *http://www.itworld.com/big-datahadoop/267396/big-data-analytics-may-detect-infection-clinicians*.

[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 generally* Tene & Polonetsky, *supra* note 6; World Economic Forum, *Unlocking the Value of Personal Data: From Collection to Usage* (Feb. 2013), *available at* http://www3.weforum.org/docs/WEF_IT_UnlockingValuePersonalData_CollectionUsage_Report_2013.pdf.

[8] *See* World Economic Forum, *supra* note 7, at 3-4.

[9] *See, e.g.*, VIKTOR MAYER-SCHÖNBERGER & KENNETH CUKIER, BIG DATA: A REVOLUTION THAT WILL TRANSFORM HOW WE LIVE, WORK, AND THINK 153 (2013) ("With big data, the value of information no longer resides solely in its primary purpose. . . . [I]t is now in secondary uses. This change undermines the central role assigned to individuals in current privacy laws.");

[10] Centre for Information Policy Leadership, *supra* note 4, at 13 ("Because big data may serve purposes that can be revealed only through the knowledge discovery phase of analytics, organisations either will not be able to describe in their notices to what purpose data will be put, or will be forced to articulate that purpose so broadly as to lack meaning.").

still obey privacy principles that protect consumers. I usually talk about these issues with industry leaders or policymakers in Washington, and I advocate for legal regimes and industry best practices that improve consumer privacy protections. But I've come to realize that we need more than law and more than "best practices" to safeguard privacy effectively. We also need new technological solutions to enhance consumer privacy.

Which brings me to you. Many of you are engineering students and professors, company chief technology officers, and computer scientists. This is your technological revolution. But you understand that technology brings challenges too and I believe that you are passionate about finding solutions. Policymakers like me and my FTC colleagues need to work hand-in-hand with you in the engineering and scientific communities. This is your "call to arms" – or perhaps, given who you are, your "call to keyboard" – to help create technological solutions to some of the most vexing privacy problems presented by big data.

Of course, you won't be like Gary Cooper in *High Noon*, fighting the outlaws all on your own. The world of big data is not quite the Wild West. We have important rules in place governing the ways certain kinds of data can be used. One is the Fair Credit Reporting Act, or "FCRA." And it is the FCRA that presents the first set of challenges for technologists to address.

First Challenge: The Fair Credit Reporting Act

The FCRA was our nation's first "big data" law. The seeds for it were planted in the aftermath of World War II. As the economy began to grow, businesses formed cooperatives to enable quicker and more accurate decisions about creditworthiness by sharing information about consumers who were in default or delinquent on loans.[11] Over time, these agencies combined, paving the way for consumers to gain access to credit, insurance and jobs. As credit bureaus increased their ability to draw inferences and make correlations through ever-larger databases, unease about the amount of information that credit bureaus held – as well as its accuracy and its use – also increased. To respond to these concerns, in 1970 Congress passed the Fair Credit Reporting Act.

FCRA governs the use of information to make decisions about consumer credit, insurance, employment and housing. Entities collecting information from multiple sources and selling it to companies making these important decisions must ensure the information is as accurate as possible and used only for approved purposes. Not only does FCRA regulate the use of consumer data, it also gives consumers important rights: Consumers are entitled to access their data, challenge its accuracy, and be notified when they are denied credit or get a loan at less than favorable rates because of negative information in their files.

[11] *See* Mark Furletti, *An Overview and History of Credit Reporting* (Payment Cards Center, Federal Reserve Bank of Philadelphia, June 2002), at 3-4.

My agency, the Federal Trade Commission, enforces the FCRA. Of course, we bring enforcement actions against traditional credit bureaus.[12] Increasingly, though, we are focusing on data brokers that collect information about consumers from offline and online sources, including social media, and then develop and sell apps and other online services for employment and tenant screening, criminal background checks, and other activities plainly covered by FCRA.[13]

FCRA is not a panacea. The process of collecting data, and synthesizing that data into profiles relating to individual consumers, is too error-prone for too many Americans.[14] The FTC's study of the accuracy of credit reports found that the reports for one in twenty U.S. consumers – 10 million people – had serious errors that could result in them receiving less favorable credit than they deserve. We all know it can be a long, arduous and extremely exasperating effort to correct a faulty credit report. Consider Julie Miller, an Oregon woman who spent years trying to correct her credit report, and who recently obtained an $18.4 million punitive judgment against one of the three major credit bureaus for its indifference to her plight.[15]

The time has come for the credit reporting industry to address its error rate. The algorithms and processes used by the industry to assign data to a particular individual (the Oregon Julie Miller and NOT the Vermont Julie Miller) are in need of modernization. So too is the industry's "dispute resolution" system, which fails to resolve many disputes – especially where consumers have identical or similar names.[16] New technological tools also must be developed to help consumers more easily obtain and understand their credit reports, and to give consumers a better, privacy-enhancing interface for correcting their credit information across multiple credit reporting agencies.

You can introduce this critical industry to 21st century techniques for responsible use of its big data. You can modernize the credit reporting industry's algorithms and processes in a privacy protective way, so that data about the financially responsible Julie Miller is no longer mixed up with data about her deadbeat doppelganger. You can redesign the industry's dispute

---

[12] *See, e.g., U.S. v. Certegy Check Servs., Inc.*, No. 13-cv-01247 (D.D.C. Aug. 15, 2013), *available at* http://www.ftc.gov/os/caselist/1123184/130815certegyorder.pdf (stipulated judgment and order, including $3.5 million penalty).

[13] *See, e.g.*, 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; *U.S. v. Spokeo, Inc.*, No. 12-CV-05001 (C.D. Cal. June 19, 2012), *available at* http://ftc.gov/os/caselist/1023163/120612spokeoorder.pdf (consent decree and order); Press Releases, FTC Warns Data Broker Operations of Possible Privacy Violations (May 7, 2013), *available at* http://www.ftc.gov/opa/2013/05/databroker.shtm; 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; 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.

[14] *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.

[15] See Laura Gunderson, *Equifax must pay $18.6 million after failing to fix Oregon woman's credit report*, THE OREGONIAN (July 26, 2013).

[16] Tara Siegel Bernard, *Credit Bureaus Willing to Tolerate Errors, Experts Say*, N.Y. TIMES (Aug. 3, 2013).

resolution systems so that disputes like hers are actually resolved, and not just kicked down the road. And you can develop an intuitive platform for consumers to use to correct errors in their credit reports, thus helping ensure that their corrections flow in a privacy-protective way to all major credit bureaus at once.

Second Challenge: the Internet of Things

The Internet of Things presents your second challenge. Interconnectivity is just around the corner. Connected cars will solve traffic congestion; smart grid devices will conserve money and the environment; smart refrigerators will tell you when you're running out of milk and, perhaps more importantly, beer; and connected medical devices will enable earlier detection and smarter treatments, saving lives.

Yet the Internet of Things presents new challenges to consumer privacy. Many connected devices have no user interface, and consumers may not even realize that the device they are using is connected, let alone sending data to third parties. All of this raises two key questions: first, without an interface, how can a company provide effective notice about the data it collects and how that data is used? And second, should society permit the data harvested from interconnected devices to be combined with other online and offline data, creating mega-profiles that have very rich details about each of our behavior – including when we do our laundry, when we raid the fridge, and when we fail to turn out the lights?[17]

The engineers and technologists who design these devices and their systems of data collection will have to rise to the challenge of making sure that the Internet of Things respects consumer privacy. Last year, the Federal Trade Commission set forth a new general privacy framework for companies and policymakers[18] that urges all companies handling consumer data to design privacy protections into their products and services – called "privacy by design". We also urged companies to use simple, "just in time" privacy disclosures that would tell consumers how information is being collected and used and give consumers the ability either to say "no" to the practice or to not engage in the transaction.

You can design connected devices with these best practices in mind. You can:

- Ensure that these connected devices build in privacy from the start.
- Make sure that the device collects no more data than is necessary for the device's functioning and that the data is held securely and for the minimum time necessary.
- Ensure that consumers are given simplified notice – even if the device has no interface – by creating a consumer friendly online dashboard that explains

[17] 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.

[18] FED. TRADE COMM'N, PROTECTING CONSUMER PRIVACY IN AN ERA OF RAPID CHANGE: RECOMMENDATIONS FOR BUSINESSES AND POLICYMAKERS (Mar. 26, 2012), *available at* http://www.ftc.gov/os/2012/03/120326privacyreport.pdf [hereinafter FTC, 2012 PRIVACY REPORT]

> through pictures, graphs or other simple terms the data the device collects about consumers, the uses of the data, and who else might see the data. The smartphones and tablets we all carry – and soon smart watches and connected glasses – create a ready canvas for immersive apps that will provide a new way of giving notice and consent that is more meaningful and less confusing for users.

Third Challenge: Increased Transparency Mechanisms

I've saved the toughest challenge for last: the vast amount of data collection and profiling that occurs by entities that are not consumer facing. These entities, called data brokers, merge vast amounts of online and offline information about consumers, turn this information into profiles, and market this information for purposes that may fall outside the FCRA. There are three categories of data brokers' practices worth focusing on.

First, there are those who are selling consumer-specific data for purposes 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.[19] Or consider the eBureau, a company that prepares rankings of potential customers based on their "occupation, salary and home value to spending on luxury goods or pet food, … with algorithms that their creators say accurately predict spending."[20] These "e-scores" are sold to determine the customers that are worth wooing on the web.[21]

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 when financial institutions – banks, credit and debit card providers, insurers – send targeted ads to targeted consumers advertising certain rates that the institution would be willing to give the consumer based on the e-score, a consumer may never know that she is eligible for an even better rate. These ads are certainly the first cousin, if not closer kin, of firm offers of credit governed by the FCRA. Yet 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.

Second, there is another class of decisions increasingly based on big data – what the FTC has called "eligibility" determinations – that could also – if founded on inaccurate information – do real harm to consumers.[22] These include determinations about whether a consumer is too risky to do business with, has engaged in fraud, or is ineligible to enroll in certain clubs, dating services, schools, or other programs. Though any of these decisions could deeply affect

---

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

[20] 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.

[21] *Id.*

[22] FTC, 2012 PRIVACY REPORT, at 68 –70.

consumers, the data used and algorithms employed do not necessarily fall within the confines of the FCRA.

Third, there is the collection and use of big data to make sensitive predictions about consumers, such as those involving their sexual orientation, health conditions, and religion.

Let's look at the well-known, even infamous, example of Target's big-data-driven campaign to identify pregnant customers through an analysis of consumers' purchases at its stores, a so-called "pregnancy prediction" score.[23] 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 expectant mom's loyalty by offering coupons tailored to her stage of pregnancy.

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. And I am not suggesting that, had Target done so, it 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 information that, by itself, is innocuous, involving routine transactions – store purchases, web searches, and social media posts – and sell that information to marketers and others.

And actually, you don't have to imagine it. The Financial Times recently highlighted[24] how some data brokers collect personal details so intimate they make Target's efforts seem tame. 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.

Undoubtedly Target 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 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 governs the use of sensitive health data for certain purposes, and will argue that if data brokers aren't employing health condition predictions 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.

---

[23] 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.

[24] 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.

In a hospital or medical trial, or some other context where our federal health privacy law, known as HIPAA,[25] applies, this argument has some force. But when health information flows outside the protected HIPAA environment, I worry about three things. First, how sensitive health information can be used to make decisions about eligibility that fall outside the contours of the FCRA, without notice to the consumer or an opportunity to challenge the accuracy of the data used to make the decisions. Second, what happens if sensitive health information falls into the wrong hands through a data breach? And third, what damage 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?

One way to solve this problem is to ensure that the health data are truly deidentified. Of course, merely stripping identifiers such as names and addresses is not sufficient; it is too easy to re-identify data. But a standard that requires companies to make it impossible to re-identify data could make it effectively useless. FTC has developed best practices around deidentification[26] that strike an appropriate balance by requiring companies to employ reasonable efforts to de-identify data, to publicly commit to use that data only in their de-identified form, and to impose legal requirements to make sure any downstream recipients of de-identified data agree not to re-identify them. And you can join the corps of computer scientists that continue to upgrade deidentification techniques.[27]

But more robust deidentification will not solve the problem of big data profiling. The entire data broker enterprise is aimed at developing greater insight into the activities, status, beliefs, and preference of *individuals*. The data the industry employs are therefore about or linkable to individuals – or as one of the industry's trade associations just-released report refers to it – "individual-level consumer data".[28]

Another solution offered to the challenges big data presents to privacy is the creation of the "algorithmist" – a licensed professional with ethical responsibilities for an organization's appropriate handling of consumer data.[29] But the algorithmist will only thrive in a firm that thoroughly embraces "privacy by design," from the engineers and programmers all the way up to the C-suite, and understands that the use of algorithms to make decisions about individuals has legal and ethical dimensions. NYU Poly and other top notch engineering and computer science schools cover ethics in their courses, but the schools and profession should require more

---

[25] 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* Dep't of Health and Human Svcs., Office of Human Research Protections, *Institutional Review Board Guide Book* at Chapter 3 (last updated 1993), *available at* http://www. hhs.gov/ohrp/archive/irb/irb_guidebook.htm.

[26] *See* FTC, 2012 PRIVACY REPORT, at 21.

[27] *See, e.g.*, Cynthia Dwork, *A Firm Foundation for Private Data Analysis*, 54 COMMS. OF THE ACM 86-95 (2011), *available at* http://research.microsoft.com/pubs/116123/dwork_cacm.pdf, and references cited therein.

[28] 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/files/2013/10/The-Value-of-Data-Consequences-for-Insight-Innovation-and-Efficiency-in-the-US-Economy.pdf .

[29] MAYER-SCHÖNBERGER & CUKIER, *supra* note 9, at 180 – 182 (2013).

systematic ethical training for undergraduate and graduate degrees. Law schools do this, and you don't ever want to be accused of lagging behind lawyers in terms of ethical training!

Unfortunately, even if industry embraces privacy by design and we license all of you as a new cadre of algorithmists, we will not have met the fundamental challenge of big data in the marketplace: that is, consumers' loss of control of their most private and sensitive information.

Changing the law would help. When I talk about these issues in Washington, 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.

But together we can begin to address consumers' loss of control over their most private and sensitive information even before legislation is enacted. I 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. And you – the engineers, computer scientists, and technologists – you can help industry develop this robust system for consumers.

The concept is simple. Through creation of consumer friendly online services, 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.

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 – the 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.

Some in industry responded quickly and positively to Reclaim Your Name. The nation's largest data broker, Acxiom, has taken the first meaningful step by launching its web-based tool, "About the Data."[30] The website allows consumers to view portions of their marketing profile

[30] *See generally* Natasha Singer, *Acxiom Lets Consumers See Data It Collects*, N.Y. TIMES (Sept. 4, 2013), at B6, *available at* http://www.nytimes.com/2013/09/05/technology/acxiom-lets-consumers-see-data-it-collects.html?pagewanted=all

by seeing certain categories of information, like personal characteristics, home, vehicles, household finances (including credit), purchases, and interests.

Consumers can correct this information. And importantly, consumers can suppress any of the data they see. This is a valuable option; if you don't want to correct erroneous data, or you simply don't want things like your income, race, or marital status to be used in your marketing profile, you can tell Acxiom to stop using it. Consumers can also opt out of Acxiom's marketing profile system altogether.

But there is still more work to do. Acxiom's site provides some transparency, but does it show consumers all the marketing information that's relevant? One reviewer reported that the current site "leaves out many data elements that Acxiom markets to its corporate clients."[31] Moreover, though the option to suppress data is valuable, consumers would have trouble finding it. Allowing consumers to suppress data more easily would be a welcome improvement. Consumers also should not mistake suppression or an opt-out for deletion or the end of data collection. Although Acxiom will not use suppressed data for marketing purposes, the data will stay put. Perhaps most importantly, Acxiom's site currently only shows consumers their data used for marketing purposes. Acxiom holds many other data sets used for eligibility and other key decisions about consumers. Acxiom should take similar steps to provide more transparency about these data sets as well.

Still, I believe Acxiom is on the right road. And you can work with Acxiom to bring it farther down this road, and with other data brokers to help them take the first necessary steps. And then, you can develop an industry-wide, one-stop shop to enable consumers to easily find out who the major data brokers are, and what choices they offer with respect to access, suppression and correction of their data.

My "call to arms" to technologists is not meant as an abdication of the responsibility that law enforcement, policy makers, Congress, industry and other stakeholders have to address these issues. We all have a vital role to play. But it is important to recognize that you – the computer scientists, the engineers, the programmers, the technologists – have a unique set of skills that are key to solving these critical privacy issues. If you join me in this effort, I think that together we can help big data operate in a system that respects consumer privacy and engenders consumer trust, allowing big data to reach its full potential to benefit us all.

Thank you.

[31] *See id.*; *see also* Bant Breen, *Misadventures in Transparency: Data Site Comes Up Short*, DIGIDAY (Sept. 30, 2013), *available at* http://digiday.com/platforms/misadventures-in-transparency-data-site-comes-up-short/.