The Trees and the Forest: Protecting Consumer Trust in the Big Data Era

U.S. Federal Trade Commissioner Julie Brill
U.S. Chamber of Commerce Foundation Conference on
The Future of Data-Driven Innovation
October 7, 2014

Thank you, Governor McKernan, for your introduction, and thank you to the Chamber of Commerce Foundation for inviting me. The focus of today's event, the future of data-driven innovation, captures a lively and ongoing conversation within the Federal Trade Commission; among consumers and businesses; and between governments around the world. I am pleased to have the opportunity to share my thoughts with you this morning.

I hope you all got a chance to get outside today. It is a glorious fall day out there. It makes me want to ask everyone to gather up their notebooks and follow me out to Lafayette Park for the rest of the speech, like my hipper college professors used to do around this time of year. Of course, I am a Vermonter, and Vermonters are hard wired to love autumn. And it is hard not to at this time of year, when the leaves are at their peak from the Acadia National Park to the Blue Ridge Parkway.

I was back in Vermont about a week ago, enjoying the leaves and working on this speech, and it occurred to me how big data is like an autumnal vista – a sea of millions of individual leaves merging into a powerful and unique interpretation of a mountainside or swath of forest. Big data does the same – collects and parses millions and billions of bits of information to tell a story, solve a problem, or sell a product in an often powerful and unique manner.

We see it everywhere these days. Local and national governments are deploying big data to tackle policy objectives like kickstarting their economies or reducing infant mortality. Traffic safety engineers are redesigning our road system and vehicles so smart cars can make our traffic smoother and our streets safer.[1] Public health agencies are predicting and managing emergencies, from the flu to Ebola, with information from big data algorithms.[2] Companies like Starbucks and the fast food chain Wendy's are locating their stores based on cyber-sifting through troves of demographic information.[3]

There is no doubt that there are great benefits to a society relying on – and an economy driven by – big data. But there are also challenges. The success of this sort of economy depends on keeping global data flows open and training a workforce that can create useful innovations out of raw data. And even more importantly, the success of this sort of economy relies on

---

[1] *See, e.g.*, Nat'l Highway Transp. Safety Admin., Advance Notice of Proposed Rulemaking Regarding Federal Motor Vehicle Safety Standards: Vehicle-to-Vehicle (V2V) Communications, 79 Fed. Reg. 49,270 (Aug. 20, 2014).

[2] Public Health Watch, *How A Computer Algorithm Predicted West Africa's Ebola Outbreak Before It Was Announced*, PUBLIC HEALTH WATCH (Aug. 10, 2014), http://publichealthwatch.wordpress.com/2014/08/10/how-a-computer-algorithm-predicted-west-africas-ebola-outbreak-before-it-was-announced/.

[3] Barbara Thau, *How Big Data Helps Chains Like Starbucks Pick Store Locations – An (Unsung) Key To Retail Success*, FORBES (Apr. 24, 2014, 8:49 AM), http://www.forbes.com/sites/barbarathau/2014/04/24/how-big-data-helps-retailers-like-starbucks-pick-store-locations-an-unsung-key-to-retail-success/.

protecting consumers from the risks to their privacy that big data can pose. As a Federal Trade Commissioner, part of my job is to take appropriate action when such risks turn into unfair or deceptive acts or practices. But as businesses, you need to be concerned about losing your customers' trust if the big data analytics on which you rely cannot handle consumers' private information with sensitivity and respect.

Some argue that big data is so revolutionary that we should not worry so much about consumer protection until we have had a chance to see where data-intensive business models might go.[4] That would be a mistake. The promise of these models depends on adopting data practices that respect not only the law but also a more expansive set of norms and consumer expectations. If you will let me indulge in another arboreal analogy, with respect to big data, I think we're at a point similar to the dawn of electronic commerce, when economists Carl Shapiro and Hal Varian warned that focusing too "heavily on the trees of technological change" could lead companies to miss the forest of basic economic forces.[5] While certain "trees" – a new web browser or new services for providing online access to stock quotes or baseball scores, for example – drove lots of media coverage and excitement in the stock market, it was the surrounding forest of interconnection, dependence on competitors, reductions in the costs of collecting and producing information, and other fundamental economic forces that determined which companies prevailed.[6]

So it is with consumer trust. If you are fixed on collecting more data, developing more refined analytics, finding ever more precise measures of your business – including your customers – you might lose sight of some of the fundamental expectations that consumers have in doing business with you. But that doesn't have to be the case. To avoid being mesmerized by the individual trees of data, companies need to step back and take a broader view that includes not only their legal obligations but also a more nuanced picture of how consumers expect their data to be treated.

Why Trust Matters to the Data-Driven Economy

Before turning to the most urgent challenges to consumer trust, and suggesting ways that companies can maintain it, let's be clear about what trust means and why it is an important economic force. According to some scholars, trust is the inverse of risk. Whereas risk asks about the chances of something going wrong, trust is the belief – but not certainty – that a person, company, or device will do what an individual expects, and not something else.[7] Trust

---

[4] *See, e.g.*, EXEC. OFFICE OF THE PRESIDENT: PRESIDENT'S COUNCIL OF ADVISORS ON SCI. & TECH., REPORT TO THE PRESIDENT: BIG DATA AND PRIVACY: A TECHNOLOGICAL PERSPECTIVE (2014), *available at* http://www.whitehouse.gov/sites/default/files/microsites/ostp/PCAST/pcast_big_data_and_privacy_-_may_2014.pdf [hereinafter BIG DATA AND PRIVACY]; Craig Mundie, *Privacy Pragmatism: Focus on Data Use, Not Data Collection*, 93 FOREIGN AFFAIRS 28, 29 (2014) (arguing that "the era of 'big data' . . . has rendered obsolete the current approach to protecting individual privacy and civil liberties" and that regulators and lawmakers should "shift[] the focus from limiting the collection and retention of data to controlling data at the most important point—the moment when it is used").

[5] CARL SHAPIRO AND HAL R. VARIAN, INFORMATION RULES 2 (1999).

[6] *See* SHAPIRO AND VARIAN, *supra* note 5, at 1-18.

[7] *See* NATIONAL ACADEMY OF SCIENCES, TRUST IN CYBERSPACE (ed. Fred B. Schneider) (1999) (discussing trust in the context of IT systems). *See also* Ashwin Jacob Mathew and Coye Cheshire, *The New Cartographers:*

might be as simple as the belief that a mobile app will protect your password when you log in or your credit card number when you make a purchase. But trust can also allow much more complex and critical relationships, such as the Internet's routing infrastructure, to function efficiently and reliably.[8] The benefit in both cases is the same: parties that trust each other do not need to go to the time and expense of verifying that the other one will do what is expected.

When consumers trust a company, for example, they are willing to use the company's services without knowing (or even understanding) every jot and tiddle of the company's data policies and practices. In this light, we can see why trust is immensely valuable but also fragile. If the company betrays this trust, it can tarnish the entire relationship. Consumers will rightly ask, "Why did I ever trust this company?" Trust is like a good reputation. It may take a long time to build, but, as the great American philosopher Will Rogers noted, you can lose it in a minute.[9]

Many companies understand this dynamic and work hard to maintain consumers' trust. With respect to consumer data, this requires constant effort, as risks to consumer information constantly shift as technologies and business practices rapidly change.

Main Challenges to Consumer Trust in the Data Driven Economy

Many of the consumer protection issues that the FTC addresses through law enforcement, policy initiatives, and education closely follow questions of trust in the data driven economy. For example, the FTC is asking whether consumers' money is safe as companies develop mobile payment mechanisms.[10] And we ask whether parents are able to exercise appropriate control over information collected from their children online.[11] More broadly, we examine whether companies keep consumers' information reasonably secure and appropriately protected.[12]

Trust and Social Order Within the Internet Infrastructure, *in* PROCEEDINGS OF THE 38TH RESEARCH CONFERENCE ON COMMUNICATIONS, INFORMATION, AND INTERNET POLICY (TPRC) (2010), *available at* http://people.ischool.berkeley.edu/~coye/Pubs/ConferenceProceedings/mathew_cheshire_2010.pdf ("Trust is an expectation of favorable reciprocity from others in situations that are uncertain or risky.").

[8] *See* Mathew and Cheshire, *supra* note 7, at 2 (arguing that "social relationships and the maintenance of trust" among administrators of inter-domain routing information "are essential for safeguarding the stability of the Internet").

[9] *See* Will Rogers Quotes, GOODREADS (last visited Oct. 1, 2014), *available at* http://www.goodreads.com/quotes/140216-it-takes-a-lifetime-to-build-a-good-reputation-but.

[10] *See* FTC, WHAT'S THE DEAL? A FEDERAL TRADE COMMISSION STUDY ON MOBILE SHOPPING APPS (staff report) (Aug. 2014) 11-15, *available at* http://www.ftc.gov/system/files/documents/reports/whats-deal-federal-trade-commission-study-mobile-shopping-apps-august-2014/140801mobileshoppingapps.pdf (reviewing pre-download disclosure regarding liability limitations and dispute resolution in mobile apps that allow consumers to make in-store purchases).

[11] *See generally* FTC, Children's Online Privacy Protection Rule, 16 C.F.R. part 312 (implementing the Children's Online Privacy Protection Act, 15 U.S.C. § 6501 *et seq.*); FTC, MOBILE APPS FOR KIDS: DISCLOSURES STILL NOT MAKING THE GRADE (staff report) (Dec. 2012), *available at* http://www.ftc.gov/sites/default/files/documents/reports/mobile-apps-kids-disclosures-still-not-making-grade/121210mobilekidsappreport.pdf; FTC, MOBILE APPS FOR KIDS: CURRENT PRIVACY DISCLOSURES ARE DISAPPOINTING (staff report) (Feb. 2012), *available at*

These are all important questions, and there are many more of them. But I will focus on the last question about privacy and data security, because I believe it is the biggest challenge to consumer trust in the data driven economy.

Data Security

Let me begin with data security. Data security has been a priority of the FTC for more than a decade. Our initial enforcement efforts focused on the financial harms that consumers could suffer when information about their credit cards or bank accounts fell into the wrong hands.[13] But, in recent years, we have made it clear that data security is essential to privacy, and unexpected revelations about our health,[14] our families,[15] our location,[16] or activities in our homes[17] can cause substantial harm to consumers.[18] As a result, data security remains one of the FTC's top priorities, not only because we continue to see one massive data breach after

---

http://www.ftc.gov/sites/default/files/documents/reports/mobile-apps-kids-current-privacy-disclosures-are-disappointing/120216mobile_apps_kids.pdf.

[12] *See generally* FTC, 2014 Privacy and Data Security Update (June 2014), *available at* http://www.ftc.gov/system/files/documents/reports/privacy-data-security-update-2014/privacydatasecurityupdate_2014.pdf (providing an overview of the FTC's privacy and data security enforcement, policy, consumer outreach, and business guidance activities from January 2013 through March 2014).

[13] *See, e.g.*, The TJX Cos., Inc., No. C-4227 (F.T.C. July 29, 2008) (consent order), *available at* http://www.ftc.gov/enforcement/cases-and-proceedings/cases/2008/08/tjx-companies-inc-matter; Dave & Buster's, Inc., No. C-4291 (F.T.C. May 20, 2010) (consent order), *available at* http://www.ftc.gov/enforcement/cases-and-proceedings/cases/2010/06/dave-busters-incin-matter; DSW, Inc., No. C-4157 (F.T.C. Mar. 7, 2006) (consent order), *available at* http://www.ftc.gov/enforcement/cases-and-proceedings/cases/2006/03/dsw-incin-matter; *BJ's Wholesale Club, Inc.*, No. C-4148 (F.T.C. Sept. 20, 2005) (consent order), *available at* http://www.ftc.gov/enforcement/cases-and-proceedings/cases/2005/09/bjs-wholesale-club-inc-matter.

[14] *See* GMR Transcription Servs., No. C-4482 (F.T.C. Aug.14, 2014) (consent order), *available at* http://www.ftc.gov/system/files/documents/cases/140821gmrdo.pdf; CBR Sys., Inc., No. C-4400 (F.T.C. Apr. 29, 2013) (consent order), *available at* http://www.ftc.gov/sites/default/files/documents/cases/2013/05/130503cbrdo.pdf.

[15] *See* TRENDnet Inc., No. C-4426, 2014 WL 556262 (F.T.C. Jan. 16, 2014) (consent order), *available at* http://www.ftc.gov/system/files/documents/cases/140207trendnetdo.pdf.

[16] *See* FTC, PROTECTING CONSUMER PRIVACY IN AN ERA OF RAPID CHANGE: RECOMMENDATIONS FOR BUSINESSES AND POLICYMAKERS 58–59 (2012), *available at* http://www.ftc.gov/sites/default/files/documents/reports/federal-trade-commission-report-protecting-consumer-privacy-era-rapid-change-recommendations/120326privacyreport.pdf (stating that "individualized location data is sensitive").; Goldenshores Techs., LLC, No. C-4446, at ¶ 7 (F.T.C. Mar. 31, 2014) (complaint), *available at* http://www.ftc.gov/system/files/documents/cases/140409goldenshorescmpt.pdf (alleging that location information is sensitive); *id.* (consent order), *available at* http://www.ftc.gov/system/files/documents/cases/140409goldenshoresdo.pdf.

[17] *See TRENDNet*, *supra* note 15.

[18] The FTC has recognized this broader set of privacy harms in cases that do not involve security breaches. *See, e.g.*, Aaron's, Inc., No. C-4442 (F.T.C. Mar. 10, 2014), *available at* http://www.ftc.gov/system/files/documents/cases/140311aaronsdo.pdf; DesignerWare, LLC, No. C-4390 (F.T.C. Apr. 11, 2013), *available at* http://www.ftc.gov/sites/default/files/documents/cases/2013/04/130415designerwaredo.pdf.

another,[19] but also because data security is an essential part of the Fair Information Practice Principles.[20] Put simply – and as the Chamber recognizes in its new report released today[21] – there is no privacy without appropriate data security. Whether consumers want to keep information entirely to themselves or share a photo with their friends and family but not their officemates, they cannot exercise the control they desire unless companies deliver on data security.

And now we are connecting cars, appliances, and many household devices to form an Internet of Things. We are starting to discover that vulnerabilities in these connected devices can reveal highly sensitive information. The first case that the FTC brought involving the Internet of Things was against a company that made Internet-connected video cameras.[22] We alleged that the company's cameras were vulnerable to having their feeds hijacked.[23] And, indeed, around 700 private video feeds, some of which included images of children and families going about their daily activities in their homes, were hacked and publicly posted as a result of the company's allegedly lax security practices.[24]

Looking more broadly, I am concerned that some of the data security lessons of the recent past aren't being applied to these exciting new technologies. A recent study by Hewlett-Packard found that 90 percent of connected devices are collecting personal information, and 70 percent of them are transmitting this data without encryption.[25] As more devices become connected to the Internet, the potential grows for more information about the most intimate details of our lives to slip into the wrong hands – and to leave other consumer devices and accounts vulnerable – unless appropriate security safeguards are put into place.

---

[19] *See, e.g.*, Jessica Silver-Greenberg, Matthew Goldstein, and Nicole Perlroth, *JPMorgan Chase Hacking Affects 76 Million Households*, N.Y. TIMES DEALBOOK (Oct. 2, 2014, 12:50 PM), *available at* http://dealbook.nytimes.com/2014/10/02/jpmorgan-discovers-further-cyber-security-issues/; Robin Seidl, *Home Depot's 56 Million Card Breach Bigger Than Target's*, WALL ST. J. (last updated Sept. 18, 2014, 5:43 PM), *available at* http://online.wsj.com/articles/home-depot-breach-bigger-than-targets-1411073571; Brian Krebs, *The Target Breach, by the Numbers*, KREBS ON SECURITY (May 6, 2014), *available at* http://krebsonsecurity.com/2014/05/the-target-breach-by-the-numbers/.

[20] *See* FTC, PROTECTING CONSUMER PRIVACY IN AN ERA OF RAPID CHANGE, *supra* note 5, at 3; EXEC. OFFICE OF THE PRESIDENT, CONSUMER PRIVACY IN A NETWORKED WORLD: A FRAMEWORK FOR PROTECTING PRIVACY AND PROMOTING INNOVATION IN THE DIGITAL GLOBAL ECONOMY 19 (Feb. 2012), *available at* http://www.whitehouse.gov/sites/default/files/privacy-final.pdf.

[21] U.S. CHAMBER OF COMMERCE FOUNDATION, THE FUTURE OF DATA-DRIVEN INNOVATION 15-16 (2014).

[22] *See* FTC, Press Release, FTC Approves Final Order Settling Charges Against TRENDNet, Inc. (Feb. 7, 2014), *available at* http://www.ftc.gov/news-events/press-releases/2014/02/ftc-approves-final-order-settling-charges-against-trendnet-inc.

[23] TRENDNet, Inc., No. C-4426 (F.T.C. Feb. 7, 2014) (complaint), at ¶ 8, *available at* http://www.ftc.gov/system/files/documents/cases/140207trendnetcmpt.pdf.

[24] *Id.* at ¶¶ 9-11.

[25] Hewlett-Packard, *Internet of Things Research Study* 2 (July 2014), *available at* http://h20195.www2.hp.com/V2/GetDocument.aspx?docname=4AA5-4759ENW&cc=us&lc=en.

Sensitive Information

A second challenge to consumer trust comes from the collection and use of sensitive personal information. Here in the United States I believe we've reached a general consensus, reflected in HIPAA and elsewhere, that personal information about health is deeply sensitive. Its inappropriate disclosure can cause severe embarrassment, harm an individual's job and other economic prospects, or reveal information about family members. Of course, HIPAA mainly covers traditional health care providers and insurers.[26] Yet some of the most exciting prospects for society-changing innovations come from wearable devices and mobile apps that encourage consumers to collect and store their own health data – placing the information collected – some of it highly sensitive – outside the current boundaries U.S. law.[27]

While the prospects of employing user generated health information from wearable devices and the like to solve health care and other societal problems in the near future are exciting, some companies are putting this information to more immediate and mundane uses. As FTC staff recently reported, some mobile health apps transmit personal information to third parties such as advertising networks and analytics companies.[28] FTC staff reviewed twelve health-related mobile apps and found that the apps transmitted information –some of it relating to sensitive health conditions such as pregnancy – to more than seventy third parties.[29] For example, one app transmitted health-related search terms, such as "ovulation" and "pregnancy," to third parties.[30] In many instances, third parties received information about consumers' workouts, meals, or diets that was identified by a real name, email address, or other unique and persistent identifiers.[31] These third parties could generate inferences that are further enriched by other data from smart devices – including location, lifestyle, and consumption habits – before consumers even know that their devices are connected to the internet.

Such surprisingly personal disclosures are at odds with consumer trust. I believe that realizing all the potential benefits of health data analytics will require us – policymakers, companies, research institutions and other stakeholders – to work to ensure strong, effective

---

[26] Health Insurance Portability and Accountability Act, Pub. L. No.104-191, 110 Stat. 1936 (1996) (codified in scattered sections of 18, 26, 29, and 42 U.S.C.).

[27] *See, e.g.*, Comments of Joy Pritts, Transcript of the FTC Seminar on User Generated and User Controlled Health Data 35-36 (May 7, 2014), *available at* http://www.ftc.gov/system/files/documents/public_events/195411/2014_05_07_consumer-generated-controlled-health-data-final-transcript.pdf (stating that "[w]e are trying to move from a paradigm in where health care is just provided on an episodic basis and really treat the patient more holistically" but "[w]hat happens then is . . . we are actively encouraging people to move their information potentially out of a HIPAA-protected bubble into the hands of others who may not be subjected to HIPAA").

[28] *See* Jared Ho, Comments at Federal Trade Commission Consumer Generated and Controlled Health Data Seminar 26–27 (May 7, 2014), *available at* http://www.ftc.gov/system/files/documents/public_events/195411/2014_05_07_consumer-generated-controlled-health-data-final-transcript.pdf.

[29] *See id.* at 25.

[30] *Id.* at 26.

[31] *Id.* at 27.

protections for health information, even when created by individuals through their apps and connected devices.

Discrimination and Unethical Data Practices

The third challenge to consumer trust that I want to highlight comes from the possibility of unfair or unethical treatment as companies use increasingly powerful analytics tools on the massive amounts of data that are available about individual consumers. This is a challenge that *all* companies need to take seriously.

Let me begin with data brokers, which are companies that collect and distribute information about consumers behind the scenes, without interacting directly with consumers. A report that the FTC released earlier this year discusses how data brokers collect an enormous amount of detail about consumers and create individual profiles about them that may contain thousands of data points.[32] Our report also showed that some of these profiles separate consumers according to race, ethnicity, family status, and other characteristics that companies are not allowed to consider for purposes such as housing, credit, employment, and medical care. Examples of segments with apparent ethnic dimensions include "Metro Parents," comprised of single parents who are "primarily high school or vocationally educated" and are handling the "stresses of urban life on a small budget"; and "Timeless Traditions," which includes immigrants who "speak[] some English, but generally prefer[] Spanish."[33]

In the marketing context that these profiles are intended to serve, merely collecting such information might not present a legal problem under current law. Indeed, these and other big data tools have the potential to promote economic inclusion. For example, big data driven marketing can make underserved consumers aware of opportunities for credit and other services.[34]

But there is also a clear potential for use of the information to be harmful and discriminatory, and to destroy consumer trust. The same data that allows banks to reach traditionally unbanked, financially vulnerable populations could just as easily be used to target them with advertisements for high-interest payday loans.[35]

---

[32] *See* FTC, DATA BROKERS: A CALL FOR TRANSPARENCY AND ACCOUNTABILITY iv (2014), *available at* http://www.ftc.gov/system/files/documents/reports/data-brokers-call-transparency-accountability-report-federal-trade-commission-may-2014/140527databrokerreport.pdf (reporting that one data broker has "3000 data segments for nearly every consumer").

[33] *Id.* at 20 n.52.

[34] *See* FTC, Conference Description, Big Data: A Tool for Inclusion or Exclusion?, http://www.ftc.gov/news-events/events-calendar/2014/09/big-data-tool-inclusion-or-exclusion (last visited Sept. 5, 2014) ("[U]ses of big data are expected to create efficiencies, lower costs, and improve the ability of certain populations to find and access credit and other services."). *See also* Comment of the Chamber of Commerce of the United States on the Big Data: A Tool for Inclusion or Exclusion? Workshop 3 (Aug. 15, 2014), *available at* http://www.ftc.gov/system/files/documents/public_comments/2014/08/00021-92389.pdf (quoting with approval the FTC's conference description).

[35] *See, e.g.*, Comment of the National Consumer Law Center on the Big Data: A Tool for Inclusion or Exclusion? Workshop 2 (Aug. 15, 2014), *available at*

Moreover, consumer segments that steer clear of traditionally restricted categories could still have devastating emotional effects on consumers. Consider, for example, a list of domestic abuse victims. Such a list might be useful for companies that want to market home security devices. But I think this is a case in which the explanation that the list is "just for marketing" falls short. Consumer profiles like these should be discussed from multiple angles, including the individual data elements that they contain, how they group consumers together, and how the profiles are used in practice.

And as companies begin scrutinizing their own data – and perhaps supplementing it with information from data brokers – they also need to be on the lookout for how data can lead them into making distinctions that are ethically, if not legally, questionable. For example, what if a company analyzing its own data, in an effort to identify "good" versus "troublesome" customers, ends up tracking individuals along racial or ethnic lines? A recent *Harvard Business Review* article argues that this kind of result isn't just possible but inevitable, and all companies should think carefully about where "value-added personalization and segmentation end[s] and harmful discrimination begin[s]."[36]

These are tough challenges. Addressing them will require stakeholders to use a variety of approaches. I'd like to highlight some steps that companies and policymakers should take right now to maintain and build consumer trust as we enter the data driven economy.

Approaches for Strengthening Consumer Trust: Security, Control, Ethics

Data Security

Improving security of data that is personally identifiable or linkable to individuals is a must. While some are enthusiastic about indiscriminately collecting data now and sorting it out later, I see big security risks in this approach. Such reservoirs of data are not only attractive targets for hackers, but I also wonder how companies that adopt a casual "collect it all" approach can have a handle on their overall security risks.

A better approach – and one that is consistent with the FTC's view that risk assessments and data minimization are integral to reasonable data security practices – is for companies to take a close look at what data they have and what data they need to serve their customers. And wherever possible, companies should robustly deidentify this data, and promise to not reidentify it.[37] Some will argue that those limitations would cut off much of the promise of finding

---

http://www.ftc.gov/system/files/documents/public_comments/2014/08/00018-92374.pdf; Jeffrey Chester and Edmund Mierzwinski, Big Data Means Big Opportunities and Big Challenges: Promoting Financial Inclusion and Consumer Protection in the "Big Data" Financial Era 13 (Mar. 2014) (submitted as a comment of the Center for Digital Democracy and U.S. PIRG on the Big Data: A Tool for Inclusion or Exclusion? Workshop), *available at* http://www.ftc.gov/system/files/documents/public_comments/2014/05/00003-90097.pdf.

[36] Michael Schrage, *Big Data's Dangerous New Era of Discrimination*, HARVARD BUSINESS REVIEW BLOG NETWORK (Jan. 29, 2014, 8:00 a.m.), http://blogs.hbr.org/2014/01/big-datas-dangerous-new-era-of-discrimination/.

[37] *See* FTC, PROTECTING CONSUMER PRIVACY IN AN ERA OF RAPID CHANGE: RECOMMENDATIONS FOR BUSINESSES AND POLICYMAKERS 21-22 (2012), *available at* http://www.ftc.gov/sites/default/files/documents/reports/federal-trade-commission-report-protecting-consumer-privacy-era-rapid-change-recommendations/120326privacyreport.pdf.

unexpected nuggets in the mountains of personal or linkable data that companies are increasingly capable of collecting, storing, and analyzing. A question that I would ask is whether these somewhat speculative benefits are worth the costs that could come from more severe breaches.

Companies would also do well to find ways to make security tools more user-friendly. As connected devices become more pervasive, companies will need to find ways to present interfaces that consumers can easily use, or make sure that secure settings are on by default.

Individual Control

Giving individuals better ways to control the privacy of their information is another way to strengthen trust in the data driven economy. After all, the notion of trust is incompatible with a relationship that one party doesn't choose to form and cannot get out of. For over a year, I have been urging companies to recognize that individual control and transparency for personal information is an enduring expectation and a much broader concept than simply permitting or refusing information collection at one point in time.[38] Through my "Reclaim Your Name" initiative, I have called on data brokers to empower consumers, through easy-to-use portals, to find out how brokers are collecting and using their data; give them access to information that data brokers have amassed about them; allow them to opt-out or correct information used for marketing purposes; and provide them the opportunity to correct errors in information used for substantive decisions.[39] These choices would allow consumers to keep aspects of their private lives away from big data driven marketing – something that will be increasingly important as more and more sensitive information about consumers becomes available.

Ethical Data Practices

But consumers cannot manage all of this on their own. Companies should also ensure that their collection and use practices are consistent with a trusted relationship. I encourage companies to think about this the way engineers think about designing automobiles: while we want to give consumers better control and transparency tools that they can easily access on their dashboards, we must also ensure that companies build better protections "under the hood" to ensure ethical treatment of consumers.[40]

Government agencies and companies have devoted a tremendous amount of effort in recent years to working on the challenges of enjoying the benefits of big data analytics while

---

[38] *See generally* Julie Brill, Comm'r, FTC, Sloan Cyber Security Lecture: A Call to Arms: The Role of Technologists in Protecting Privacy in the Age of Big Data (Oct. 23, 2013), *available at* http://www.ftc.gov/sites/default/files/documents/public_statements/call-arms-role-technologists-protecting-privacy-age-big-data/131023nyupolysloanlecture.pdf; Julie Brill, Comm'r, FTC, Keynote Address at the 23rd Computers, Freedom, and Privacy Conference: Reclaim Your Name (June 26, 2013), *available at* http://www.ftc.gov/sites/default/files/documents/public_statements/reclaim-your-name/130626computersfreedom.pdf.

[39] *See id.*

[40] Yochi Dreazen, . . . *Guard Your Privacy: Steps to Protect Confidentiality While Online Are Often Underused*, WALL ST. J. (Nov. 18, 2002, 9:52 AM), *available at* http://online.wsj.com/articles/SB1037222318310696668 (quoting Marc Rotenberg as saying, "I don't think users need more settings on the dashboard – they need online privacy protections under the hood.").

maintaining appropriate privacy protections. Legislation would be helpful here. I would like to see the United States strengthen its laws through baseline privacy legislation,[41] as well as data security legislation[42] and stronger requirements for data brokers.[43]

Even without additional legislation, companies can and should do more right now to define and implement data practices that will earn consumers' trust. For data brokers, assessing the potential impact of their products that profile consumers by race, ethnicity or other sensitive classifications, or that are proxies for such sensitive classifications, would be a strong, proactive step. Data brokers should find out how their clients are using these products, tell the rest of us what they learn about these actual uses, take steps to ensure any inappropriate uses cease immediately, and develop systems to protect against such inappropriate uses in the future.

And, as I mentioned, companies that are beginning to dive into their own data should also be thinking carefully about and acting on these issues. Some meaningful actions could include deploying greater resources and imagination to designing intuitive portals, dashboards, and better interfaces for consumers to use to control their privacy and security. Companies could also make ethics reviews part of their big data analytics business practices – perhaps by creating "consumer subject review boards" to identify and reduce consumer risks, as one U.S. privacy scholar has suggested.[44] And whether or not companies go to this level of formality, every one of them should be asking whether their analysis of consumer data is taking them into questionable territory.[45]

* * * * * *

If there are any serious gardeners out there, you know that the richest soil to be found anywhere is on the floor of a mature forest. Those beautiful leaves in the Vermont vista I talked about at the beginning of the speech will eventually brown and fall and deliver minerals and nutrients back to the tree and to new seedlings come spring. If the leaves are removed, the forest weakens and dies. There is a lesson there. The data driven economy will not thrive unless the bits of consumer information collected and analyzed are used to benefit the consumer – plowed back into the relationship between businesses and their customers to make it stronger, deeper, and ultimately more profitable. That means winning customers' trust by treating their privacy and private data with care, honesty, and respect. If that happens, I believe a comprehensive

---

[41] EXEC. OFFICE OF THE PRESIDENT, CONSUMER PRIVACY IN A NETWORKED WORLD, *supra* note 4, at 1.

[42] *See* FTC, Prepared Statement on Protecting Personal Consumer Information from Cyber Attacks and Data Breaches Before the Senate Committee on Commerce, Science, and Transportation 10-12 (Mar. 26, 2014), *available at* http://www.ftc.gov/system/files/documents/public_statements/293861/140326datasecurity.pdf.

[43] FTC, DATA BROKERS: A CALL FOR TRANSPARENCY AND ACCOUNTABILITY viii-ix, (2014), *available at* http://www.ftc.gov/system/files/documents/reports/data-brokers-call-transparency-accountability-report-federal-trade-commission-may-2014/140527databrokerreport.pdf.

[44] *See generally* Ryan Calo, *Consumer Subject Review Boards: A Thought Experiment*, 66 STAN. L. REV. ONLINE 97 (Sept. 3, 2013), *available at* http://www.stanfordlawreview.org/online/privacy-and-big-data/consumer-subject-review-boards.

[45] *See* Michael Schrage, *Big Data's Dangerous New Era of Discrimination*, HARVARD BUSINESS REVIEW BLOG NETWORK (Jan. 29, 2014, 8:00 a.m.), http://blogs.hbr.org/2014/01/big-datas-dangerous-new-era-of-discrimination/.

vision of “data for good” will be at hand, as consistent and welcome and powerful as fall’s foliage spectacle.

Thank you.