It's Getting Real: Privacy, Security, and Fairness by Design in the Internet of Things
Carnegie Mellon University
January 28, 2015

Thank you, President Suresh, for that kind introduction, and thank you Lorrie for inviting me to today's Data Privacy Day celebration. It's great to be here at Carnegie Mellon, which has had a hand in shaping so many of our leaders in technology and science, including 12 Turing Award winners. You are the engineers and computer scientists who already are, or will soon be, colonizing the astonishing new world of the Internet of Things. I was lucky enough to attend the Consumer Electronics Show earlier this month, and I was bowled over by the products on display, and I mean that quite literally. One of a pair of synchronized dancing drones I was watching crashed in the middle of its pirouette. It was still a supremely impressive and strangely beautiful demonstration.

And, oh the connected devices! I finished up my 2015 Christmas list eleven months early: Swarovski pendants and bracelets that double as health monitors; smart cars that steer you out of trouble before you even know you're in it; sprinklers that conserve water; front doorbells that send a video of your visitor to your smart phone; garages that alert you when your teenager has left the door open – again; and outdoor grills that text you when it's time to turn the meat.

Okay, maybe that last one is not exactly a necessity. But if you happen to married to someone who regularly turns New York Strips into naugahyde, it could change your life. I'm kind of counting on it.

The benefits we might draw from the Internet of Things are real and significant. Convenience is just one of them. Besides making our lives easier and more entertaining, connected devices will give us tremendous insights through data – lots of data. Six years ago, for the first time, the number of "things" connected to the Internet surpassed the number of people connect to the Internet.[1] The amount of data in the world has already been doubling every two years. Experts estimate that, as of this year, there will be 25 billion connected devices and by 2020, 50 billion.[2] The data that we collect from the Internet of Things, and the insights we draw from this data could help solve some of the big challenges that we face as a society. In the hands of scientists and analysts, data from sensors in our cars,[3] in our homes, and on our wrists could help us find ways to use energy more efficiently, avoid traffic jams, and stay

[1] DAVE EVANS, CISCO INTERNET BUS. SOLUTIONS GRP., THE INTERNET OF THINGS: HOW THE NEXT EVOLUTION OF THE INTERNET IS CHANGING EVERYTHING 3 (2011), *available at* http://www.cisco.com/web/about/ac79/docs/innov/IoT_IBSG_0411FINAL.pdf. These estimates include all types of connected devices, not just those aimed at the consumer market.

[2] *Id.*

[3] *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).

healthier longer and with less expense. Public health emergencies, from the flu to Ebola, will be predicted and managed with information from Big Data crunching computer algorithms.[4]

So what's the catch? Much of this data will be deeply personal, and say a great deal about us as individuals. We already know that every time we swipe our smartphone screens to check Twitter or tap our phones to pay for coffee, we add to the swelling rivers of data that capture the details of what we do, what we buy, what we read, and where we go. Soon these streams of data will reveal whether we're at home and what we're doing there. They will record how much we've exercised, when we've gained a few pounds, and how well we sleep. They'll log our vital signs, and help us manage our diabetes, heart and other health conditions.

At the same time, as Google's Chairman, Eric Schmidt, reportedly said last week in Davos, "the Internet will disappear."[5] That is, we'll all carry, wear, sit next to, and use so many devices that are connected all the time that the idea of a "network connection" will become an anachronism. Just as you forget about shifting gears in your car once you have an automatic transmission, Schmidt predicts that you'll forget about devices being in a connected state. Connectivity will just be part of how things work

We are on the threshold of the Age of Omniscience, when everyone can know everything about everyone – and share that knowledge in real time with everyone else over our omnipresent devices. The burgeoning Internet of Things is our entryway. Some say we should stride through, confident that the future is a bright one, a golden age.

But what about privacy? What about concerns regarding how this deeply personal information will be used to form rich portraits of each of us? Many have looked at the increasing numbers of connected devices, and the corresponding explosion in the amount of data we have, and concluded that "privacy is dead."[6] Others have taken a slightly different angle and stated that the privacy principles that the FTC and many agencies, companies, and advocates support need to be abandoned and replaced with a different framework.[7]

I could not disagree more. It is certainly true that the Internet of Things, big data, and new forms of analytics all challenge traditional privacy principles. The challenges at the top of

---

[4] 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/.

[5] Chris Matyszczyck, *The Internet Will Vanish, Says Google's Eric Schmidt*, CNET (Jan. 22, 2015, 6:00 PM), *available at* http://www.cnet.com/news/the-internet-will-vanish-says-googles-schmidt/.

[6] *See* Richard Carter, *Privacy is Dead, Harvard Professors Tell Davos Forum*, YAHOO! NEWS (Jan. 22, 2015, 9:46 AM), *available at* http://news.yahoo.com/privacy-dead-harvard-professors-tell-davos-forum-144634491.html; Polly Sprenger, *Sun on Privacy: "Get over It"*, WIRED (Jan. 26, 1999), *available at* http://archive.wired.com/politics/law/news/1999/01/17538 (quoting former Sun Microsystems CEO Scott McNealy as saying to a group of reporters and analysts: "You have zero privacy anyway. Get over it.").

[7] *See* FTC, INTERNET OF THINGS: PRIVACY & SECURITY IN A CONNECTED WORLD 19-22 (2015) (staff report), *available at* http://www.ftc.gov/system/files/documents/reports/federal-trade-commission-staff-report-november-2013-workshop-entitled-internet-things-privacy/150127iotrpt.pdf (discussing views of workshop participants) [IOT REPORT].

the list are data security, the collection and use of sensitive information, and the fair and ethical use of data. However, as our report on the Internet of Things, issued just yesterday makes clear, the right response to these challenges – for regulators, companies, technologists, and advocates – is to figure out not *whether*, but *how* to address them in the always-on, massively connected world that we're developing.[8] In order to fully reap the benefits of the Internet of Things and Big Data, both must be imbued with tested principles of privacy.

I believe we can unlock the potential of Big Data and enjoy its benefits while still obeying the privacy principles that protect individuals – the same principles that we at the Federal Trade Commission have championed for many years through a combination of law enforcement and policy development.[9] Finding solutions that honor privacy principles will be important – and not just to the FTC and the consumers that we protect. It will also be critical to companies who know that they need to maintain consumers' trust if they are going to win their loyalty and business.[10]

This alignment creates an opportunity for you in the audience today. Some of you are today's leading engineering professors, company chief technology officers, and computer scientists; and others of you are studying to fill those roles in the not too distant future. The Internet of Things is your technological revolution. And you understand that technology like this brings challenges, and I believe that you are passionate about finding solutions. You have the skills that are necessary to find out when systems are unreasonably vulnerable to security breaches or are picking up more information than they need for their expected purpose. You have the ability to think about whether algorithms might be treating some consumers in an unfair or exclusionary manner. And – just as importantly – you have the ability to do better, much better, by designing privacy, security, and fairness into the Internet of Things from the very beginning.

Data Security

Let me begin with data security. Data security has been a priority of the FTC for more than a decade. The FTC has obtained more than 50 consent orders against companies that, in our view, misrepresented how good their security was or failed to take reasonable measures to protect consumer data.[11] Our initial enforcement efforts focused on the financial harms that consumers could suffer when their Social Security numbers or information about their credit

---

[8] *See generally id.*

[9] *See generally* FTC, PROTECTING CONSUMER PRIVACY IN AN ERA OF RAPID CHANGE: RECOMMENDATIONS FOR BUSINESSES AND POLICYMAKERS (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.

[10] *See, e.g.*, Mark Penn, *Views from around the globe: 2nd Annual Report on How Personal Technology is Changing our Lives*, THE OFFICIAL MICROSOFT BLOG (Jan. 19, 2015), *available at* http://blogs.microsoft.com/blog/2015/01/19/views-around-globe-2nd-annual-report-personal-technology-changing-lives/ (reporting on a survey that finds that privacy "is one persistent concern about personal technology that nearly everybody expresses").

[11] *See* FTC, Commission Statement Marking the FTC's 50th Data Security Settlement (Jan. 31, 2014), *available at* http://www.ftc.gov/system/files/documents/cases/140131gmrstatement.pdf.

cards or bank accounts fell into the wrong hands.[12] But we have also focused on security lapses that harmed consumers in other ways, for instance by disclosing medical information;[13] pharmaceutical records;[14] and information about our families,[15] our location,[16] or activities in our homes.[17]

Moreover, reasonable data security is essential to privacy. Put simply, there is no privacy without appropriate data security. Several of our recent cases drive this point home.

For instance, consider our recent action against Snapchat.[18] We alleged that Snapchat deceived consumers by representing that the messages consumers sent through the app would "disappear forever" after a few seconds.[19] However, the Snapchat app was vulnerable in ways that allowed the recipient of a message to bypass the app's security measures and permanently store messages.[20] Even if you're not a Snapchat user, you can imagine that a security failure that

---

[12] *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.

[13] *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.

[14] *See* FTC, Press Release, Rite Aid Settles FTC Charges That It Failed to Protect Medical and Financial Privacy of Customers and Employees (July 27, 2010), available at http://www.ftc.gov/news-events/press-releases/2010/07/rite-aid-settles-ftc-charges-it-failed-protect-medical-and; FTC, Press Release, CVS Caremark Settles FTC Charges: Failed to Protect Medical and Financial Privacy of Customers and Employees; CVS Pharmacy Also Pays $2.25 Million to Settle Allegations of HIPAA Violations (Feb. 18, 2009), *available at* http://www.ftc.gov/news-events/press-releases/2009/02/cvs-caremark-settles-ftc-chargesfailed-protect-medical-financial.

[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] *See* FTC, Press Release, Snapchat Settles FTC Charges That Promises of Disappearing Messages Were False (May 8, 2014), *available at* http://www.ftc.gov/news-events/press-releases/2014/05/snapchat-settles-ftc-charges-promises-disappearing-messages-were.

[19] Snapchat, No. C-4501, at ¶ 3 (F.T.C. Dec. 23, 2014), *available at* http://www.ftc.gov/system/files/documents/cases/141231snapchatcmpt.pdf.

[20] *Id.* ¶¶ 6-19.

leads to the capture of an image that you thought would be ephemeral is a pretty rude shock and undermines a central selling point of the app.

Similarly, consider our recent cases against Credit Karma and Fandango. We alleged that these apps were vulnerable to "man-in-the-middle" attacks, in which a hacker could pose as a legitimate data recipient and collect highly sensitive information, such as credit card details, credit report data, and Social Security numbers.[21] Credit Karma and Fandango are now both prohibited from misrepresenting the privacy and security of their products, and required to establish comprehensive programs designed to address security risks.[22]

Some companies trade in other types of highly sensitive information. For example, debt brokers are entities that buy information about consumers who have unpaid debts and sell them to collectors. Debt portfolios not only list debtors by name – and thus reveal who has unpaid debts, a fact that can be sensitive on its own[23] – but these portfolios also may contain full bank account numbers and other sensitive financial information. Last year, the FTC sued two debt brokers for posting debt portfolios containing information about tens of thousands of consumers on publicly accessible websites, free for anyone to download.[24] The Commission alleged that this was an unfair disclosure of consumers' information, because it was likely to cause substantial harm that consumers could not avoid and provided no offsetting benefits to consumers or competition.

And the first data security case that the FTC brought involving the Internet of Things also raised privacy concerns. In this case, we alleged that the defendant company's Internet-connected cameras were vulnerable to having their feeds hijacked.[25] 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.[26]

---

[21] FTC, Press Release, Fandango, Credit Karma Settle FTC Charges That They Deceived Consumers by Failing to Securely Transmit Sensitive Personal Information (Mar. 28, 2014), *available at* http://www.ftc.gov/news-events/press-releases/2014/03/fandango-credit-karma-settle-ftc-charges-they-deceived-consumers.

[22] *See* Credit Karma, Inc., No. C-4480 (F.T.C. Aug. 13, 2014) (decision and order), *available at* http://www.ftc.gov/system/files/documents/cases/1408creditkarmado.pdf; Fandango, LLC, No. C-4481 (F.T.C. Aug. 13, 2014) (decision and order), *available at* http://www.ftc.gov/system/files/documents/cases/140819fandangodo.pdf.

[23] *See* Fair Debt Collection Practices Act, 15 U.S.C. § 1692 *et seq.* (associating abusive debt collection practices with "personal bankruptcies, to marital instability, to the loss of jobs, and to invasions of individual privacy").

[24] *See* FTC v. Bayview Solutions, LLC, Case 1:14-cv-01830-RC (D.D.C. Aug. 27, 2014), *available at* http://www.ftc.gov/system/files/documents/cases/111014bayviewcmp.pdf *and* FTC v. Cornerstone and Co., LLC, Case 1:14-cv-01479-RC (D.D.C. Aug. 27, 2014), *available at* http://www.ftc.gov/system/files/documents/cases/141001cornerstonecmpt.pdf. The courts in both cases have entered preliminary injunctions against the defendants.

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

[26] *Id.* at ¶¶ 9-11.

Part of the solution to these data security issues will be enacting new laws. President Obama visited the FTC just two weeks ago and, while there, called on Congress to enact strong, flexible, and technology-neutral federal legislation to strengthen the FTC's existing data security enforcement tools, and to provide notification to consumers when there is a security breach. We at the FTC most recently reiterated this call in our new report on the Internet of Things. General data security legislation, including the authority to issue rules and seek civil penalties from companies that violate the law, should protect against unauthorized access to personal information, and should also protect device functionality itself. The latter could become an issue if, for example, a device like a pacemaker is hacked,[27] a case in which both health information could be compromised and the person wearing the device could be seriously harmed.

While legislation and FTC enforcement actions are important responses to the data security threats posed by the expanding Internet of Things, the first line of defense will be the actions that companies need to take to secure their connected devices, as well as the data gathered, compiled, and shared through the Internet of Things.

It is you, the technologists and engineers designing the next generation of connected devices, who we must count on to protect security by pumping it into the very heart of these products. That is not going to be easy, and we have a long way to go. 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.[28] Traditional consumer goods manufacturers entering the Internet of Things market, unlike technology firms, have not spent decades thinking about how to secure their products and services from hackers.[29] Furthermore, the small size and light weight of many connected devices could inhibit encryption and other robust security measures.[30] Some connected devices will be cheap and essentially disposable, with limited computing power. If a vulnerability is discovered on such a device, it may be difficult – from both an engineering and an economic perspective – for the manufacturer to update the software or provide a patch – or to get news of such a fix to consumers.

The Internet of Things report advises that companies adopt a policy of security by design, wiring security into their products at the outset, rather than as an afterthought.[31] Technologists working on new devices should perform initial security risk assessments, test services for security flaws before they go to market, continuously monitor products throughout the life cycle,

---

[27] *See* Barnaby Feder, *A Heart Device Is Found Vulnerable to Hacker Attacks*, N.Y. TIMES (Mar. 12, 2008), *available at* http://www.nytimes.com/2008/03/12/business/12heart-web.html.

[28] 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.

[29] Brian Fung, *Here's the Scariest Part of the Internet of Things*, WASH. POST (Nov. 19, 2013), *available at* http://www.washingtonpost.com/blogs/the-switch/wp/2013/11/19/heres-the-scariest-part-about-the-internet-of-things/.

[30] Stacey Higginbotham, *The Internet of Things Needs a New Security Model, Which One Will Win?* GIGAOM (Jan. 22, 2014), *available at* https://gigaom.com/2014/01/22/the-internet-of-things-needs-a-new-security-model-which-one-will-win/.

[31] IOT REPORT, *supra* note 7, at 28.

and, to the extent possible, patch known vulnerabilities.[32] Companies should train all employees about good security; implement reasonable access control measures to limit the ability of an unauthorized person to access a consumer's device, data, or even the consumer's network; and ensure that security issues are addressed at the appropriate level of responsibility within the organization.[33] When companies identify significant risks within their systems, they should implement a defense-in-depth approach, implementing security measures at multiple levels.[34]

Of course, data minimization also plays a key role in promoting data security and privacy. You can't lose or misuse what you don't have, and for that reason, the FTC has long pushed companies to practice data minimization. We renew this call in our report on the Internet of Things, suggesting that companies limit the consumer data they collect and maintain to the information they truly need, and dispose of the information once they no longer need it.[35] We also call on companies to deidentify the data they do keep.[36] From the FTC's perspective, effective deidentification combines reasonable technical deidentification with accountability measures that prohibit the company that controls the data from attempting to reidentify it, and places the same prohibitions on any recipients of the deidentified data.[37] The role for technologists here is clear: You can help design the connected devices and apps that do the most with the least amount of personally linkable information, and ensure that the devices and apps regularly flush their stores of unnecessary data.

Sensitive Data

Let me turn to the second privacy challenge coming from the Internet of Things: the collection and use of sensitive personal information. Here in the United States I believe we've reached a general consensus, reflected in HIPAA[38] – our federal health privacy law – 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. HIPAA mainly covers traditional health care providers and insurers. 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 of U.S. law.

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. Yet some companies are putting this information to more immediate and mundane uses. As FTC staff

[32] *Id.* at 28-29.

[33] *Id.*

[34] *Id.* at 30.

[35] *Id.* at 33-39.

[36] *Id.* at 37-39.

[37] *Id.* at 38.

[38] 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.).

recently reported, some mobile health apps transmit personal information to third parties such as advertising networks and analytics companies. FTC staff reviewed twelve health-related mobile apps and found that they transmitted information – some of it relating to sensitive health conditions such as pregnancy – to seventy-six third parties.[39] For example, one app transmitted health-related search terms, such as "ovulation" and "pregnancy," to third parties. In many instances, third parties received information about consumers' workouts, meals, or diets identified by a real name, email address, or other unique and persistent identifiers.[40] These third parties could combine this information with other data from smart devices – including location, lifestyle, and consumption habits – to generate additional sensitive inferences.

Such surprisingly personal disclosures are at odds with consumer trust. Yet I often hear that it's too difficult to put traditional privacy safeguards in place. Wearable fitness devices, for example, might not have a user interface to serve as a means to present consumers with a choice about data collection. Devices will become too numerous for consumers to manage their information. And that information is too valuable to consider deleting. These arguments often lead their proponents to the conclusion that the only feasible privacy safeguard for sensitive information generated through the Internet of Things will be through risk-based frameworks that focus exclusively on how sensitive data is actually used.

I think it is important that we break these arguments down, and address them carefully. First, as to the argument that traditional privacy principles, such as notice, choice, and data minimization, are unrealistic to apply to the Internet of Things, I frequently urge 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. Connected devices are no different, but providing transparency and control will require some creative thinking. Immersive apps and websites should be employed, to describe to consumers in meaningful and relatively simple terms the nature of the information being collected, and to provide consumers with choices about whether any of this information can be used by entities or persons who fall outside the context in which the consumer is employing the device, and in which the consumer expects her information to remain private. Another promising tool for providing consumer choice is the "command center" that companies are now developing to run multiple household connected devices.[41] The driving force here is convenience, but these command centers could also provide an opportunity for consumers to understand the information their devices are generating, and to control where that information goes. After all, if you can have a centralized interface to program your garage door, thermostat, television, refrigerator, and who knows what else, you ought to be able to use that interface to make meaningful choices about the data your devices will collect and where they'll send it.

---

[39] *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.

[40] *Id.* at 26.

[41] *See* Don Clark, *The Race to Build Command Centers for Smart Homes*, WALL ST. J. (Jan. 5, 2015), *available at* http://www.wsj.com/articles/the-race-to-build-command-centers-for-smart-homes-1420399511.

Second, it is quite helpful for companies to develop practices that examine how they use data. But I don't believe that we can rely entirely on such "use-based" frameworks to protect consumers privacy. A lack of transparency is one drawback to a use-based model. Unless permissible uses have been specified in a way that's accessible to everyone – in legislation, for example – it will be difficult or impossible for consumers to understand what's happening with their data.[42] Focusing solely on the risks and benefits of data uses could also lead companies to ignore the risks created by data collection and retention on their own.[43] One such risk is that the vast amounts of data that companies collect will become an attractive target for hackers, and the risk of harm to consumers from a security breach increases along with the amount of data that companies store.[44] Another risk is that companies will collect lots of sensitive information about consumers, or infer it from other data that they collect.[45] Even if companies don't make further use of such sensitive data, I believe that its collection or creation through inference is something that consumers will want to know about and be able to control.

Data Brokers, Big Data, and Using Data Fairly

Security and privacy are not the only challenges for policymakers and technologists that come from the Internet of Things. We at the FTC are also wrestling with questions raised by the ever-improving ability of algorithms to make inferences and predictions about us. These algorithms have been around in one guise or another for a long time, but their power will swell if the profiles that analytics companies generate grow richer with information from connected devices.

Data brokers – firms unknown to most consumers – collect and combine compendia of tens of thousands of bits of data about each of us, and morph them into startlingly accurate profiles.[46] When run through the big data mill, these data points can be woven together into predictions about personal behavior and characteristics.[47] These profiles are quite valuable to data brokers' clients, who want to know where we live, where we work, how much we earn – as well as our daily activities (both offline and online), and our interests. But they can also contain inferences about more sensitive attributes, such our race, our health conditions, and our financial status. Data brokers may describe us as "Financially Challenged" or perhaps having a "Bible Lifestyle."[48] They may place us in a category of "Diabetes Interest" or "Smoker in Household."[49] Some of them sell marketing lists that identify consumers with addictions or AIDS. Others focus on ethnicity and finances, creating consumer lists such as "Metro Parents"

[42] *See* IOT REPORT, *supra* note 7, at 42.

[43] *Id.* at 43.

[44] *See id.*

[45] *See id.*

[46] 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 (defining "data broker") [DATA BROKER REPORT].

[47] *Id.* at 20 & n.52; *id.* at 25 & n.57.

[48] *Id.* at 20 n.52, 21.

[49] *Id.* at 46, 55.

(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" (immigrants who "speak[] some English, but generally prefer[] Spanish").[50]

To see an example of how such targeting can be harmful in practice, consider our recent case against a company called LeapLab. In a complaint that we filed last month against LeapLab, the Commission alleged that the company sold information about consumers who applied for payday loans to two kinds of customers.[51] About five percent of the applications went to bona fide lenders.[52] The rest, the vast majority, went to non-lenders, some of whom used the information to commit fraud.[53] We alleged that these disclosures were unfair – and illegal.

Of course, in this case, LeapLab knew that consumers were interested in payday loans. But some other company might just as well have created – through data analytics or based on a data brokers' profile – a list of consumers who were likely interested in a payday loan. Such a list could be used in a way that benefits those consumers. For example, a bank might use such a list to target their advertising for safe, low-cost, entry level financial products, because such consumers might be more likely to be unbanked or financially vulnerable. But the same list could just as easily be used by other less scrupulous firms to target consumers with high-cost, short-term loans that lead consumers into a cycle of debt. Both uses are, in some sense, "marketing," but the outcomes for consumers who receive the bank's ads could be quite different from those who receive ads from payday lenders.

Data from the Internet of Things will add depth and precision to inferences about what we want and what we do. I'm confident that many responsible companies will take a close look at whether their analysis and use of all of this data leads them to categorize consumers by race, ethnicity or other sensitive classifications, or proxies for such sensitive classifications. 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.[54] Computer and data scientists will play a crucial role in such ethics reviews, by helping to determine whether specific analytics practices pose risks of excluding, or otherwise placing at a disadvantage, groups defined according to sensitive traits. But as I just noted, I don't think it's sufficient to rely solely on companies to decide whether classifications – and their uses of them – are good or bad.

---

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

[51] FTC v. Sitesearch Corp., d/b/a LeapLab (D. Az. Dec. 23, 2014) (complaint), *available at* http://www.ftc.gov/systems/files/documents/cases/141223leaplabcmpt.pdf.

[52] *Id.* at ¶ 18.

[53] *Id.* ¶¶ 19-23.

[54] *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.

Baseline privacy legislation would help address many of these underlying issues. So would data broker legislation, which could place some transparency, access and correction requirements on data brokers, as well as their sources of information and their clients.[55]

But there are steps that companies can and should take now, and technologists who understand predictive analytics could make these steps even more meaningful.

I'd like to see all companies that are engaged in data analytics that generate sensitive information about consumers deploy greater resources and imagination to designing intuitive portals, dashboards, and better interfaces for consumers to use to control their privacy and security. Companies should provide consumers with creative tools that would give them the opportunity to learn about their marketing profiles, so they can learn whether their race, health conditions, or financial status are part of their marketing profiles, and make meaningful choices about that. And consumers should be able to learn about profiles used for more substantive decisions – like whether they are potentially "risky" customers – so they can correct inaccuracies that might lead to inappropriate conclusions.

And computer engineers can play a critical role in designing such portals and other mechanisms for providing consumers with such meaningful information and control tools.

* * * * *

I am one of those lucky people who has had the great fortune to spend a career doing what I love – using the law to protect consumers. But I have to admit to being a tad jealous when I look at the careers you have or are about to start. As technologists, algorithmists, CIOs, and computer scientists, you are standing at the forefront of a social and technological revolution that is changing and will change our world in miraculous ways. Riding the wave of the Internet of Things and Big Data, you are ushering in the Age of Omniscience and, to a great extent, your work will determine whether this new Age shines brightly or fades to black.

Fidel Castro once said, "Revolution is a struggle to the death between the future and the past." At the risk of throwing a pall over our recent détente with Cuba, I would like to take issue with that. The success of the revolution – your revolution – that we are talking about today, I believe, depends on the extent to which the technology of the future embraces the proven privacy principles of the past. As policymakers like me forge ahead to develop guidelines, best practices and legislative recommendations on how to secure consumers' data and protect their privacy in this Age of Omniscience, we need you figure out how to wire security and privacy into the devices and algorithms that will define this new age. Engendering consumer trust in the Internet of Things will allow us all to realize its full promise. I'm confident that if we work together, we will achieve that goal.

[55] *See* DATA BROKER REPORT, *supra* note 46, at 49-54 (discussing the Commission's legislative recommendations with respect to marketing, risk mitigation, and people search products).