Fordham Law Review

Volume 83 *Volume 83*
Issue 1 *Volume 83, Issue 1*

Article 6

2014

The Internet of Things: Building Trust and Maximizing Benefits Through Consumer Control

Julie Brill
U.S. Federal Trade Commission

Recommended Citation
Julie Brill, *The Internet of Things: Building Trust and Maximizing Benefits Through Consumer Control*, 83 Fordham L. Rev. 205 (2014).
Available at: http://ir.lawnet.fordham.edu/flr/vol83/iss1/6

This Essay is brought to you for free and open access by FLASH: The Fordham Law Archive of Scholarship and History. It has been accepted for inclusion in Fordham Law Review by an authorized administrator of FLASH: The Fordham Law Archive of Scholarship and History. For more information, please contact tmelnick@law.fordham.edu.

ESSAY

THE INTERNET OF THINGS: BUILDING TRUST AND MAXIMIZING BENEFITS THROUGH CONSUMER CONTROL

*Julie Brill**

The Internet of Things is one of the fastest growing facets of a world that is becoming more data intensive. Connecting cars, appliances, and even clothing to the internet promises to deliver convenience, safety, and, through analysis of the torrent of additional data generated, potential solutions to some of our most intractable problems. But turning on this data flood also creates privacy and security risks for consumers, challenging us to consider how to apply basic privacy principles to the Internet of Things. A wide range of stakeholders—technologists, lawyers, industry leaders, and others—has a role to play in meeting this challenge.

I. FROM PROTOTYPES TO PRICE TAGS: THE INTERNET OF THINGS IS HERE, AND SO ARE ITS PRIVACY AND SECURITY CHALLENGES ... 205
II. PRIVACY CHALLENGES OF BIG DATA AND THE INTERNET OF THINGS ... 210
III. ENSURING TRANSPARENCY AND CONTROL ON THE INTERNET OF THINGS: A JOB FOR THE ENTIRE INDUSTRY ... 213
A. The Challenge for Device and Service Providers ... 214
B. The Challenge for Data Brokers ... 215
CONCLUSION ... 217

I. FROM PROTOTYPES TO PRICE TAGS: THE INTERNET OF THINGS IS HERE, AND SO ARE ITS PRIVACY AND SECURITY CHALLENGES

We already celebrate birthdays on Facebook and share our thoughts on Twitter. We are accustomed to having our smartphones always at our sides

---

* Julie Brill is a Commissioner of the U.S. Federal Trade Commission. She thanks her attorney advisor Aaron Burstein for his invaluable assistance in preparing this article. Keynote address delivered at the Law & Information Policy Symposium, *What Is Your Car Saying to Your Shoes? Assessing the Internet of Things*, sponsored by the Fordham Center on Law and Information Policy and the Princeton University Center on Information Technology Policy held on March 14, 2014 at the Fordham University School of Law.

so that we are never out of touch with our colleagues or kids. And we know that our credit card purchases, online and in the store, are tracked.

Consumers' daily activities yield an astounding amount of data. Overall, 1.8 trillion gigabytes of data were created in the year 2011 alone—equivalent to every U.S. citizen writing three tweets per minute for almost 27,000 years.[1] Individuals are estimated to create 70 percent of all data in the world,[2] and it is predicted that the total amount of data in existence will double every two years from now on.[3] According to one report, the data broker Acxiom processes 50 trillion data transactions per year.[4] Scientists are tackling the many challenges of "extreme-scale computing,"[5] including experimenting with immersing servers in mineral oil to keep them from melting down.[6]

Perhaps more important than the rapid growth in available data is the proliferation of data sources. One company estimates that there will be 25 billion internet-connected devices by 2015[7]—an average of more than three devices for every human being on the planet[8]—and by the end of this decade, machine-to-machine communications will represent a growing share of all data, with 40 percent of all data predicted to come from sensors.[9] Our constant connections are about to become much stronger.

At the January 2014 Consumer Electronics Show in Las Vegas, companies put on a staggering display of connected devices, demonstrating that the Internet of Things is here.[10] Indeed, it will not be long before we start to ask why a given object *isn't* connected to the internet.

Consider several examples. The first is a connected baby "onesie" called the Mimo, which can monitor a baby's respiration rate, body temperature,

---

1. Lucas Mearian, *World's Data Will Grow by 50X in Next Decade, IDC Study Predicts*, COMPUTERWORLD (June 28, 2011, 1:23 PM), http://www.computerworld.com/s/article/9217988/World_s_data_will_grow_by_50X_in_next_decade_IDC_study_predicts.

2. *Big Data Is Just Beginning to Explode*, CSC, http://www.csc.com/big_data/flxwd/83638-big_data_just_beginning_to_explode_interactive_infographic (last visited Sept. 21, 2014).

3. Steve Lohr, *The Age of Big Data*, N.Y. TIMES, Feb. 12, 2012, at SR1.

4. Natasha Singer, *You for Sale: Mapping, and Sharing, the Consumer Genome*, N.Y. TIMES, June 16, 2012, at BU1.

5. *Big Data and Extreme-Scale Computing*, EXASCALE.ORG, http://www.exascale.org/bdec/ (last visited Sept. 21, 2014).

6. Jim Witkin, *Cooling a Computer Server with Mineral Oil*, N.Y. TIMES GREEN BLOG (Sept. 6, 2012, 4:37 PM), http://green.blogs.nytimes.com/2012/09/06/cooling-a-computer-server-with-mineral-oil/.

7. 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.

8. *See Current World Population*, WORLDOMETERS, http://www.worldometers.info/world-population/ (last visited Sept. 21, 2014) (reporting that the world population reached 7 billion in 2011 and is predicted to reach 8 billion in 2024).

9. *Seven Big Data Trends for 2014*, BIG DATA-STARTUPS (Dec. 19, 2013), http://www.bigdata-startups.com/big-data-trends-2014.

10. Dan Gillmor, *The Real CES Takeaway: Soon We'll Be Even More Connected and Have Even Less Privacy*, GUARDIAN (Jan. 10, 2014, 8:45 AM), http://www.theguardian.com/commentisfree/2014/jan/10/ces-takeaway-internet-of-things-privacy-concerns.

and activity level and send the data to a smart phone application.[11] According to the vendor's website, parents can configure the app to "set alerts" and even display "analytics about their baby's sleep."[12] For parents worried about sudden infant death syndrome, or simply trying to figure out how to get their infants—and themselves—to sleep through the night, such data from their own nursery might be very useful.

Figure 1. The Mimo Baby Monitor and Data Shown in Smartphone App.[13]

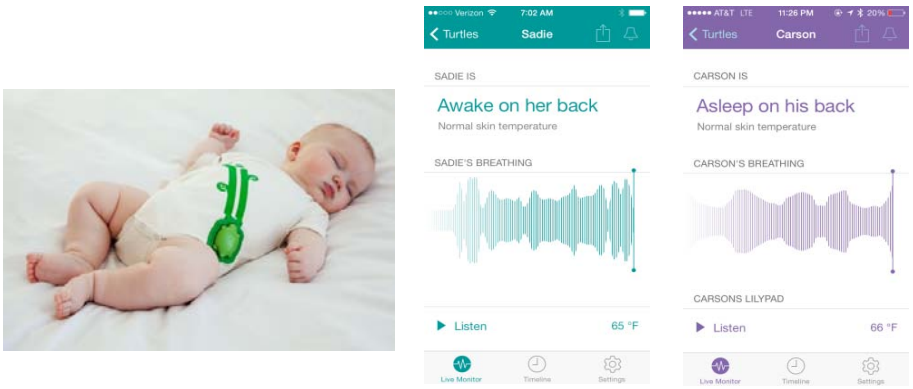
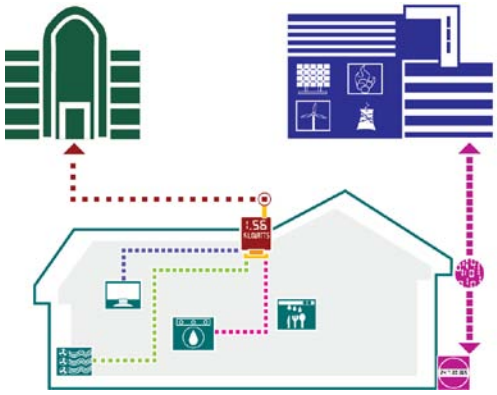


Figure 2. Devices that Could Be Internet-Connected in a Smart Home.[14]



11. *The Mimo Baby Monitor*, REST DEVICES, http://mimobaby.com/mimo/ (last visited Sept. 21, 2014).

12. *Id.*

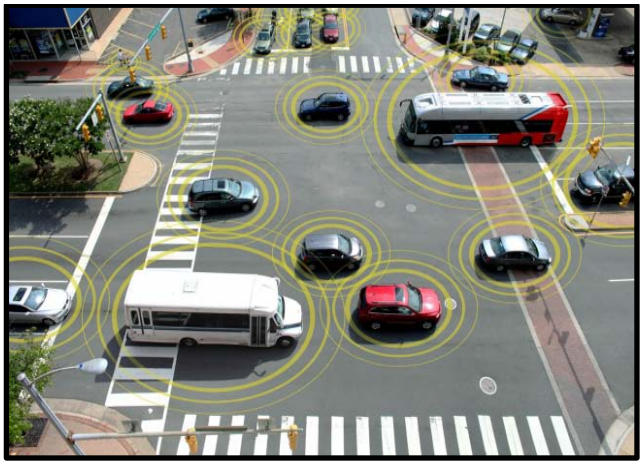
13. Source: http://mimobaby.com/mimo/. Rest Devices, which markets the Mimo baby monitor system, states explicitly that the system "is not a medical device" and "is not designed to detect or prevent causes of sudden infant death syndrome." *Mimo Baby Monitor Terms of Service*, REST DEVICES, http://mimobaby.com/terms (last visited Sept. 21, 2014).

14. Source: Brian P. Miller Photo & Design, http://www.brianpmillerphotography.com/, *reprinted in* DEIRDRE K. MULLIGAN, LONGHAO WANG & AARON BURSTEIN, PRIVACY IN THE SMART GRID: AN INFORMATION FLOW ANALYSIS 27 (2011), *available at* http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1815605.

If we are beginning to connect our kids to the internet, it is no surprise that many of the devices that consumers use each day in their homes are also becoming networked. Thermostats, refrigerators, ovens, and lighting systems are just a few of the household necessities that can communicate over a network.[15] These advances can make life more convenient for consumers. Consumers will be able to make sure that they have turned down the heat even after they have left the house for work, and getting out of bed to turn off the kitchen light might become a thing of the past.

Cars are becoming not only computers but also data sources with wheels. Already, some cars allow you to "call ahead" to start the air conditioner on a hot day, or to receive safety adjustments without ever going to the dealership.[16] One expert reported that some cars have more than 100 computers in the vehicle,[17] and manufacturers are providing consumers with the ability to run apps and connect to the internet over 4G networks.[18]

Figure 3. Schematic of Communciations Among Smart Vehicles to Avoid Collisions.[19]



15. *See* Megan Wollerton, *Smart Appliances, Connected Homes at CES 2014*, CNET (Jan. 10, 2014, 10:48 AM), http://ces.cnet.com/8301-35306_1-57616968/smart-appliances-connected-homes-at-ces-2014/.

16. Christopher Wolf, Panel Remarks at the Federal Trade Commission Internet of Things Workshop 249, 250 (Nov. 19, 2013), *available at* http://www.ftc.gov/sites/default/files/documents/public_events/internet-things-privacy-security-connected-world/final_transcript.pdf.

17. Yoshi Kohno, Panel Remarks at the Federal Trade Commission Internet of Things Workshop 242 (Nov. 19, 2013), *available at* http://www.ftc.gov/sites/default/files/documents/public_events/internet-things-privacy-security-connected-world/final_transcript.pdf.

18. *See LTE Powered M2M Connections to Surpass 200 Million, Says 4G Market Report*, 4G-PORTAL.COM (Aug. 6, 2014), *available at* http://4g-portal.com/lte-powered-m2m-connections-to-surpass-200-million-says-4g-market-report.

19. Source: DEP'T OF TRANSP., http://its.dot.gov/image_gallery/image26.htm (last updated Mar. 18, 2014, 10:27 AM).

Convenience is only part of the story. Scientists, entrepreneurs, academics, and policymakers see the potential for this vast expansion in data regarding our everyday movements and activities to solve important social challenges, from reducing the amount of gas we waste sitting in traffic jams[20] and more efficiently managing our energy consumption[21] to achieving breakthroughs in healthcare.[22] The potential societal benefits that will flow from solving these challenges are enormous and exciting.

Some of these advances are already becoming apparent in healthcare. A diverse and growing array of "wearable" devices can measure how far a person walks, how well she sleeps, and even her blood glucose levels.[23] Mobile apps allow consumers to seek information about their health and serve as a gateway between wearable devices and the internet. Together, these apps and devices promise to allow consumers to take greater control over their own health. And wearable health devices could feed data into analyses that benefit individuals and society more generally.

But consumers, policymakers, and academics also see risks in these vast storehouses of data. A recent report from McKinsey puts the privacy challenges of big data in stark terms: "Privacy has become the *third rail* in the public discussion of big data."[24] The Internet of Things shows how deeply personal information will be abundant and easily available. Connected devices will offer a detailed view of where we are, what is happening in our homes, and what our children are doing. If combined with other online and offline data, these new data sources have the potential to create alarmingly personal consumer profiles.

Now is the time to ask how companies can provide this burgeoning connectivity—and its considerable benefits—without compromising consumers' privacy or losing their trust. Will consumers know that connected devices are capable of tracking them in new ways, especially

---

20. *See* Timothy Hunter, *Traffic Jams, Cell Phones and Big Data*, UC BERKELEY AMPLAB BLOG (Jan. 18, 2012), https://amplab.cs.berkeley.edu/2012/01/18/traffic-jams-cell-phones-and-big-data/.

21. *See* Doug Peeples, *Is Big Data the Next Big Thing?*, SMARTGRIDNEWS.COM (Jan. 7, 2014), http://www.smartgridnews.com/artman/publish/Business_Analytics/Is-Big-Data-the-Next-Next-Thing-6263.html#.Uw4iTNAdY1k (quoting an industry expert who predicts that big data "will enable utilities to better plan and prepare for major events, system growth and the ensuing changes we will see as a result of low-cost natural gas with further expansion of distributed generation").

22. *See, e.g.*, Brian Proffitt, *Big Data Analytics May Detect Infections Before Clinicians*, ITWORLD (Apr. 12, 2012, 3:36 PM), http://www.itworld.com/big-datahadoop/267396/big-data-analytics-may-detect-infection-clinicians.

23. Martha Mendoza, *Google Develops Contact Lens Monitor*, SAN JOSE MERCURY NEWS (Jan. 17, 2014, 5:53 AM), http://www.mercurynews.com/business/ci_24930224/google-develops-contact-lens-glucose-monitor; Katrina Plyler, *What Is Everybody Wearing? Fitness Tech Gadgets!*, U.S. NEWS & WORLD REP. HEALTH BLOG (Apr. 11, 2014, 8:00 AM), http://health.usnews.com/health-news/blogs/eat-run/2014/04/11/what-is-everybody-wearing-fitness-tech-gadgets.

24. Brad Brown, David Court & Tim McGuire, *Views from the Front Lines of the Big Data-Analytics Revolution*, MCKINSEY & CO. (Mar. 2014), http://www.mckinsey.com/Insights/Business_Technology/Views_from_the_front_lines_of_the_data_analytics_revolution?cid=other-eml-alt-mkq-mck-oth-1403 (emphasis added).

when many of these devices have no user interface and function autonomously? How will these new sources of data flow into the huge constellation of personal data that is already collected, analyzed, sold, and used to advertise to consumers and profile them to assess the riskiness of doing business with them? How will companies address the gap between the expectations consumers have formed around "dumb" appliances and the ability of smart devices to generate accurate, abundant, and sensitive data?

An equally important set of questions surrounds data security in the Internet of Things. Protecting data from unauthorized access and disclosure is a basic element of maintaining data privacy and is paramount when sensitive data, which will undoubtedly be a significant portion of the vast amounts of data generated by the Internet of Things, is at issue. But will companies that, for decades, have manufactured "dumb" appliances take the steps necessary to keep secure the vast amounts of personal information that their newly smart devices will generate? Will companies design their devices and services to provide reasonable security not only in isolation but also as part of a highly complex and interconnected new ecosystem? An initial look at the state of the Internet of Things suggests that 90 percent of connected devices are collecting personal information, and 70 percent of them are transmitting this data over unencrypted networks.[25] This is an area that the Federal Trade Commission (FTC) is watching closely.[26]

These are some of the big data privacy and security challenges presented by the Internet of Things. Here are some specific starting points to address these challenges.

II. PRIVACY CHALLENGES OF BIG DATA AND THE INTERNET OF THINGS

One of the most troubling risks coming from the collection and use of big data is its use in making sensitive predictions about consumers, such as those involving their health conditions, sexual orientation, religion, and race. An infamous example is Target's so-called "pregnancy prediction" score.[27] Using retail transaction data, Target was able to calculate, not only *whether* a consumer was pregnant, but also *when* her baby was due.[28] It used the information to win the expectant mom's loyalty by offering coupons tailored to her stage of pregnancy.[29]

Moreover, data brokers, entities about which most people know nothing because they are not consumer-facing, are going far beyond this level of information gathering in the profiles that they develop from vast amounts of

25. *See* HP, INTERNET OF THINGS RESEARCH STUDY (2014), http://fortifyprotect.com/HP_IoT_Research_Study.pdf.

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

27. *See* Charles Duhigg, *Psst, You in Aisle 5*, N.Y. TIMES, Feb. 16, 2012, § 6 (Magazine).

28. *Id.*

29. *Id.*

online and offline data.[30] As the FTC's recent report on data brokers details, these profiles may reveal where consumers live; how much they earn; and their race, health conditions, and interests.[31] Data brokers use this information to construct marketing "segments"—categories that group consumers based on their interests and attributes, including their ethnicity, financial status, and health conditions.[32] Data organized in this way could give rise to discriminatory effects in marketing and a broad array of other commercial transactions.[33] The Government Accountability Office reported that at least one data broker includes in its consumer profiles information about twenty-eight or more specific diseases, including cancer, diabetes, clinical depression, and prostate problems.[34] According to a Senate staff report released in December 2013, another data broker keeps 75,000 data elements about consumers in its system, including the use of yeast infection products, laxatives, and OB/GYN services, among other health-related data.[35] Yet another company analyzes innocuous data from social media and other sources to predict disease conditions like diabetes, obesity, and arthritis to persuade particular consumers to join medical trials.[36] All of this creation, collection, and use of health information is happening outside of the Health Insurance Portability and Accountability Act[37] and, in fact, outside any regulatory scheme to protect this information.

It is not hard to imagine the devices mentioned earlier, or their close cousins, feeding data into this system. As FTC staff recently reported,

---

30. *See 60 Minutes: The Data Brokers: Selling Your Personal Information* (CBS television broadcast Mar. 9, 2014), *available at* http://www.cbsnews.com/news/the-data-brokers-selling-your-personal-information/.

31. *See* FTC, DATA BROKERS: A CALL FOR TRANSPARENCY AND ACCOUNTABILITY 20 n.52, 25 & n.57 (2014), *available at* http://www.ftc.gov/system/files/documents/reports/data-brokers-call-transparency-accountability-report-federal-trade-commission-may-2014/140527databrokerreport.pdf.

32. *Id.* at 20 n.52; Statement, Julie Brill, Comm'r, FTC, Data Brokers: A Call for Transparency and Accountability 3 (May 27, 2014), *available at* http://www.ftc.gov/system/files/documents/public_statements/311551/140527databrokerrptbrillstmt.pdf.

33. Brill, *supra* note 32, at 3.

34. U.S. GOV'T ACCOUNTABILITY OFFICE, GAO-13-663, INFORMATION RESELLERS: CONSUMER PRIVACY FRAMEWORK NEEDS TO REFLECT CHANGES IN TECHNOLOGY AND THE MARKETPLACE 53 (2013), *available at* http://www.gao.gov/assets/660/658151.pdf (summarizing elements of Experian marketing lists).

35. STAFF OF S. COMM. ON COMMERCE, SCI., AND TRANSP., 113TH CONG., A REVIEW OF THE DATA BROKER INDUSTRY: COLLECTION, USE, AND SALE OF CONSUMER DATA FOR MARKETING PURPOSES 12 (2013), *available at* http://www.commerce.senate.gov/public/?a=Files.Serve&File_id=0d2b3642-6221-4888-a631-08f2f255b577 (citing documentary submission from Equifax); *see also id.* at 14 (listing health care-related data elements that Equifax maintains).

36. *See* Joseph Walker, *Data Mining to Recruit Sick People*, WALL ST. J., Dec. 17, 2013, at B1 (quoting an industry official as claiming that "[w]e are now at a point where, based on your credit-card history, and whether you drive an American automobile and several other lifestyle factors, we can get a very, very close bead [sic] on whether or not you have the disease state we're looking at").

37. Pub. L. No. 104-191, 110 Stat. 1936 (1996) (codified in scattered sections of 18, 26, 29, and 42 U.S.C.).

some mobile health apps transmit personal information to third parties such as advertising networks and analytics companies.[38] 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.[39] For example, one app transmitted health-related search terms, such as "ovulation" and "pregnancy," to third parties.[40] 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.[41] 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.

There are two main reasons to be concerned about the vast amounts of personal data coming from the Internet of Things. First, we should all be concerned about the use of deeply sensitive personal information to make decisions about consumers outside a legal regime that would provide notice and an opportunity to challenge the accuracy of the data. We will pay a price every time data is inaccurate, misused, or falls into the wrong hands through a security breach. And we will pay a price in the lost sense of autonomy in a society in which information about highly sensitive aspects of our lives is available for analysts to examine without our knowledge or consent, or perhaps to the highest bidder.

Second, we should all be skeptical that questions about privacy will keep consumers away from the Internet of Things because they do not trust it. I believe that unchecked vacuuming of our information is not inevitable, that we can and should place limits on untethered collection and retention of personal information about consumers to engender their trust. Some argue that companies so clearly see the need to keep consumers' trust that they will play it safe with consumer data coming from the Internet of Things by offering strong privacy protections.[42] During our ongoing national discussion about National Security Agency surveillance, national security, and privacy, the President and other leaders at the highest levels of government, as well as leaders within the business community, have recognized that the trust of individuals is essential to the success of programs and services built on big data analytics.[43] As we have seen,

38. *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.

39. *See id.* at 25.

40. *Id.* at 26.

41. *Id.* at 27.

42. *See, e.g.*, Wolf, *supra* note 16, at 259.

43. *See* Remarks on Review of Signals Intelligence, 2014 DAILY COMP. PRES. DOC. 1, 4 (Jan. 17, 2014) ("[F]or our intelligence community to be effective over the long haul, we must maintain the trust of the American people, and people around the world."); Steve McClellan, *Sorrell: "Opt-Out" Is No Longer an Acceptable Data Strategy*, MEDIAPOST

however, from the internet of PCs, cell phones, and tablets, pressures within an industry can encourage companies to collect and share more and more personal information while weakening privacy safeguards.

The promise of the Internet of Things and big data analytics have led some to call for a shift in how we think about basic privacy principles. Proponents of "risk-based frameworks" call attention to the difficulties of refraining from collecting unnecessary data and of providing consumers with meaningful notice and choice about data collection and use.[44] These advocates argue that companies should instead focus on assessing which uses of personal data pose risks to individuals and developing appropriate safeguards.[45]

I am very much in favor of encouraging companies to think deeply about privacy risks, but it is essential for the public to be involved in decisions about data collection and use. As I discuss, that is where transparency, control, deidentification, and data minimization, adapted for the data intensive Internet of Things, come in. Any company that handles data from the Internet of Things, whether it interacts directly with consumers or provides data services in the background, should now start thinking about how to adapt these principles.

III. ENSURING TRANSPARENCY AND CONTROL ON THE INTERNET OF THINGS: A JOB FOR THE ENTIRE INDUSTRY

The privacy and data security practices that companies adopt as they build new internet-connected devices and services will have profound effects on the personal data environment that develops in this ecosystem.

Fortunately, the FTC and many others have been addressing privacy challenges as new technologies and business models—from online commerce, to behavioral advertising, to mobile devices—have rapidly

---

NEWS (Jan. 23, 2014, 1:35 PM), http://www.mediapost.com/publications/article/218015/sorrell-opt-out-is-no-longer-an-acceptable-data.html (quoting Martin Sorrell to say that businesses "are going to have to work harder to show the benefits that 'big data' brings to consumers and economies"); Brad Smith, *Time for an International Convention on Government Access to Data*, MICROSOFT ON THE ISSUES (Jan. 20, 2014), http://blogs.technet.com/b/microsoft_on_the_issues/archive/2014/01/20/time-for-an-international-convention-on-government-access-to-data.aspx (advocating for an international treaty to provide consistent privacy protections for personal data with respect to government collection of data).

44. *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) [hereinafter BIG DATA AND PRIVACY], *available at* http://www.whitehouse.gov/sites/default/files/microsites/ostp/PCAST/pcast_big_data_and_privacy_-_may_2014.pdf; 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").

45. *See* BIG DATA AND PRIVACY, *supra* note 44, at 41–42 (recommending individually defined data use preferences that travel with data); Mundie, *supra* note 44, at 14.

grown and evolved in recent years. Industry adoption of the best practices that the FTC described in its landmark 2012 Privacy Report[46] would go a long way toward providing strong and appropriate consumer privacy protections with respect to the Internet of Things.

A. The Challenge for Device and Service Providers

Three of these best practices warrant particular attention. The first is privacy by design. Because many connected devices will have little or no user interface, it is especially important for companies to promote consumer privacy in their products and services and throughout their organizations.[47] Privacy and ethical considerations are an increasingly hot topic among technologists in both industry and academia. As more universities provide their science and engineering students with additional training in ethical data collection and use, I believe that smart companies will find better ways to put privacy and ethical considerations into practice.[48]

Second, developers of connected devices should engage in robust deidentification of personal data to further ensure better privacy on the Internet of Things. The FTC's best practices for deidentification strike an appropriate balance and include both robust deidentification technologies and social agreements to not reassociate deidentified data with particular individuals.[49] This means that companies should do everything technically practicable to strip their data of identifying markers; they should make a public commitment not to try to reidentify the data; and they should contractually prohibit downstream recipients of the deidentified data from reidentifying it.[50] The technical prong of this framework poses challenges that researchers are continuing to tackle, with an eye toward the Internet of Things and beyond.[51]

Third, connected device developers should recognize that effective transparency is a fundamental building block of consumer privacy protections. The FTC recommends transparency improvements, including shorter, clearer, and more standardized notices and machine-readable

---

46. 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.

47. *See id.* at 22.

48. *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.

49. FTC, *supra* note 46, at 21.

50. *See id.*

51. The White House Office of Science and Technology Policy and MIT cohosted a workshop in early 2014. The workshop was a first in a series of events being held across the United States in response to President Obama's call for "a review of privacy issues in the context of increased digital information and the computing power to process it." *See* White House Office of Sci. and Tech. Pol'y & MIT, Big Data Privacy Workshop: Advancing the State of the Art in Technology and Practice (Mar. 3, 2014), http://web.mit.edu/bigdata-priv/index.html.

notices, which could make it easier for consumers to gain greater understanding of the nature of the data their new devices collect and transmit.[52] Others are suggesting entirely new ways of providing notice, such as through "visual, auditory or tactile cues" tailored for a specific device.[53] Going further, immersive apps or portals could help consumers gain a comprehensive view of how their devices are collecting and disclosing data.[54]

Technologists have the skills needed to make big data processing more privacy protective, to design interfaces that allow consumers to understand and exercise meaningful choices about data collection and use, and to improve the rigor and accuracy of the expanding variety of data-driven decisions that affect consumers. As some scholars have argued, however, firms may need to create more formal roles and structures to achieve a sustained focus on privacy. One proposed role is that of the "algorithmist"—a licensed professional with ethical responsibilities for the handling of consumer data.[55] Another possibility is for companies to empanel "Consumer Subject Review Boards" to determine whether projects involving consumer data are legal and ethical.[56] But the algorithmist and Consumer Subject Review Boards will only thrive in a firm that acknowledges that the use of algorithms to make decisions about individuals has legal and ethical dimensions and has everyone from the engineers and programmers all the way up to top executives thoroughly embrace the important role of "privacy by design," transparency, and other best practices to address these concerns.

B. The Challenge for Data Brokers

In addition to focusing on the developers of connected devices, we must focus on the behind-the-scenes data collectors who are creating rich profiles about consumers. If the data broker industry wants to build consumers' trust and gain the benefits of this trust, I believe that the industry needs to take some affirmative steps to change its relationship with consumers. This would be a wise investment for the industry even if the Internet of Things did not exist, but it is critical to making the industry a trustworthy participant in the data driven ventures that the Internet of Things could spawn.

---

52. FTC, *supra* note 46, at 61–64.

53. Jules Polonetsky, Director, Future of Privacy Forum, Comments on Connected Smart Technologies in Advance of the FTC "Internet of Things" Workshop 6 (May 31, 2013), *available at* http://www.ftc.gov/sites/default/files/documents/public_comments/2013/07/00013-86159.pdf.

54. *See id.*

55. VIKTOR MAYER-SCHÖNBERGER & KENNETH CUKIER, BIG DATA 180–82 (2013).

56. *See* Ryan Calo, *Consumer Subject Review Boards*, 66 STAN. L. REV. ONLINE 97 (2013); Jules Polonetsky, Omer Tene & Christopher Wolf, *How to Solve the President's Big Data Challenge*, IAPP PRIVACY PERSPECTIVES (Jan. 31, 2014), https://www.privacyassociation.org/privacy_perspectives/post/how_to_solve_the_presidents_big_data_challenge.

Legislative solutions, such as Chairman Rockefeller's and Senator Markey's Data Broker Accountability and Transparency Act,[57] would make an invaluable contribution. But the industry needs to take action even before legislation is enacted. To this end, I have urged industry to join a comprehensive initiative that I call "Reclaim Your Name."[58] Put simply, consumers should have more knowledge about and control over decisions like how much information to share, with whom, and for what purpose to reclaim their names.

The initiative would work as follows: through creation of consumer-friendly online services, "Reclaim Your Name" would empower the consumer to find out how brokers are collecting and using her data. It would 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." As the data that participating companies handle or create becomes more sensitive—for example, relating to health conditions, sexual orientation, and financial condition—the data brokers would provide greater transparency and more robust notice and choice to consumers. The 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 that all data brokers provide, and the choices consumers can make about the use of their data. Policymakers can encourage companies to devote the resources necessary to addressing the legal, ethical, and technological challenges surrounding big data. Importantly, both the White House and the FTC have recently joined my call for data brokers to adopt elements of "Reclaim Your Name." In a report released in May 2014, the White House called for data brokers to become more transparent by building a common portal that lists data brokers by name, describes their data practices, and provides ways for consumers to exercise choices about how data brokers collect and use their information.[59] The FTC has gone further by recommending legislation that would not only require data brokers engaged in marketing to create such a portal but also require them to give consumers appropriate access to their data and the ability to suppress its use.[60]

Transparency, access, and control—whether they result from data brokers' voluntary actions or legislation—are important to improving the protections for consumer data, but they are not sufficient. Accountability is another critical element of protecting the sensitive data that will find its way to data brokers through new devices as well as from more established sources, such as retailers and ordinary websites. Legislation is the best way

57. S. 2025, 113th Cong. (2014).

58. *See generally* Brill, *supra* note 48.

59. EXEC. OFFICE OF THE PRESIDENT, BIG DATA: SEIZING OPPORTUNITIES, PRESERVING VALUES 62 (2014), *available at* http://www.whitehouse.gov/sites/default/files/docs/big_data_privacy_report_may_1_2014.pdf.

60. FTC, *supra* note 31, at 49–53.

to create this accountability. Specifically, legislation should require data brokers to take reasonable steps to ensure that their original sources of information obtained appropriate consent from consumers.[61] Legislation should also require data brokers to employ reasonable procedures to ensure that their clients do not use their products for unlawful purposes.[62] Requiring data brokers to ensure that consumers have appropriately consented to the use of the data that goes into the brokers' products, and to ensure that their clients use their products within the bounds of the law and best practices, will place data brokers at the center of systems designed to ensure accountability for their products and services.[63]

CONCLUSION

Ensuring that privacy is woven into the fabric of the Internet of Things requires us not only to think carefully about what data a specific device collects but also about how that data will be used and to whom it will ultimately flow. Strong privacy and security protections will sustain the consumer trust that will help the Internet of Things and big data reach their full potential to benefit us all. Academics, technologists, lawyers who counsel companies that are building the Internet of Things, consumer advocates, and policymakers all have a role to play in developing these protections. The time to start is now.

61. *See id.*
62. *See* Brill, *supra* note 32, at 5–6.
63. *See id.*