FTC Commissioner Julie Brill
The Internet of Things: Building Trust and Maximizing Benefits Through Consumer Control

Presented at
Fordham University School of Law
Center on Law and Information Policy
What Is Your Car Saying to Your Shoes? *Assessing the Internet of Things*
New York, NY
March 14, 2014

Thank you, Joel, for that kind introduction, and thank you to the Center and the School of Law for inviting me to speak this afternoon. It is a pleasure to discuss the benefits and the consumer protection challenges of the Internet of Things with all of you.

The Internet of Things is just 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. Each of us in this diverse audience – technologists, lawyers, industry leaders, and other stakeholders – has a role to play in meeting this challenge. And the time to do it is now.

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're used to having our smartphones always at our sides so we don't miss a beat with our colleagues or kids. And we know that our credit card purchases, online and in the store, are tracked.

Our daily activities as consumers yield an astounding amount of data. Overall, 1.8 trillion gigabytes of data were created in the year 2011 alone – which is 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's predicted that the total amount of data will double every two years from now on.[3] According to one report, the data broker Acxiom

---

[1] Lucas Mearian, *World's data will grow by 50X in next decade, IDC study predicts*, COMPUTERWORLD , June 28, 2011, *available at* http://www.computerworld.com/s/ article/9217988/ World_ s_ data_ will_ grow _by_ 50X_ in_ next_ decade_ IDC_ study_ predicts?pageNumber=1.

[2] CSC, Big Data Is Just Beginning to Explode, http://www.csc.com/big_ data/flxwd/83638-big_ data_ just_ beginning_ to_ explode_ interactive_ infographic (last visited Feb. 26, 2014).

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

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, 40% of data will come from sensors.[9]

So our constant connections are about to become much stronger. In January I traveled to Las Vegas for the Consumer Electronics Show. Behind all the flash of the show and Las Vegas itself was one unmistakable message: The Internet of Things is here. Companies were showcasing their connected devices everywhere, and I began to wonder how long it will be before we start to ask why a given object *isn't* connected to the Internet.

Let me give you a few examples. The first one is a connected baby "onesie" called the Mimo, which can monitor a baby's respiration rate, body temperature, and activity level – and send the data to a smart phone app.[10] According to the vendor's website, parents can even configure the app to "set alerts" and even display "analytics about their baby's sleep."[11] For parents worried about SIDS, or simply trying to figure out how to get their infants – and themselves – to sleep through the night, data from their own nursery might be very useful.

If we're beginning to connect our kids to the Internet, it's 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 talk over a network.[12] This can make life more convenient for consumers. We'll be able to make sure we've turned down the heat even after we've left the house for work, and getting out of bed to turn off the kitchen light might become a thing of the past.

---

[4] Natasha Singer, *Mapping, and Sharing, the Consumer Genome*, N.Y. Times, at BU1, June 17, 2012, *available at* http://www.nytimes.com/2012/06/17/technology/acxiom-the-quiet-giant-of-consumer-database-marketing.html.

[5] Big Data and Extreme-Scale Computing, http://www.exascale.org/bdec/ (last visited Feb. 24, 2014).

[6] Jim Witkin, *Cooling a Computer Server with Mineral Oil*, Green: Energy, the Environment, and the Bottom Line, N.Y. TIMES, Sept. 6, 2012, *available at* http://green.blogs.nytimes.com/2012/09/06/cooling-a-computer-server-with-mineral-oil/.

[7] Dave Evans (Cisco Internet Business Solutions Group), *The Internet of Things: How the Next Evolution of the Internet Is Changing Everything*, at 3, Apr. 2011, *available at* http://www.cisco.com/web/about/ac79/docs/innov/IoT_IBSG_0411FINAL.pdf.

[8] *See* Worldometers, Current World Population, http://www.worldometers.info/world-population/ (last visited Feb. 25, 2014) (reporting that the world population reached 7 billion in 2011 and is predicted to reach 8 billion in 2024).

[9] Big Data – Startups, Seven Big Data Trends for 2014, Dec. 19, 2013, *available at* http://www.bigdata-startups.com/big-data-trends-2014.

[10] Rest Devices, The Mimo Baby Monitor, *available at* http://mimobaby.com/mimo/ (last visited Mar. 11, 2014).

[11] *Id.*

[12] *See* Megan Wallerton, *Smart Appliances, Connected Homes at CES 2014*, CNET, Jan. 10, 2014, *available at* http://ces.cnet.com/8301-35306_1-57616968/smart-appliances-connected-homes-at-ces-2014/.

Cars are becoming not only computers but also data sources with wheels. Already, some cars allow you to "call ahead" and start the air conditioner before you reach your car on a hot day, or to receive safety adjustments without ever going to the dealership.[13] One expert reported that some cars have more than 100 computers in the vehicle,[14] and manufacturers are providing consumers with the ability to run apps and connect to the Internet over 4G networks.

Convenience is only part of the story. Scientists, entrepreneurs, academics, and policy makers see the potential for this vast expansion in the data available about us to solve important social challenges, from reducing the amount of gas we waste sitting in traffic jams[15] and more efficiently managing our energy consumption,[16] to achieving breakthroughs in healthcare.[17] The potential benefits that these kinds of discoveries can bring to society are enormous and exciting.

But consumers, policy makers, and academics also see risks to consumers 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."[18] The Internet of Things shows how deeply personal information will be abundant and easily available. Connected devices will offer a detailed view into where we are, what's happening in our homes, and what our children are doing. The very nature of these devices marks a major shift for consumers, who until now have had a handful of devices that mainly serve to connect them to the Internet. Going forward, consumers will have a multitude of devices that could generate data that is accurate, abundant, and sensitive – and, if combined with other online and offline data, could 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 when many of these devices have no user interface? How will these new sources of data flow into the huge constellation of personal data that already exists? Will companies that, for

---

[13] Christopher Wolf, Transcript of FTC Workshop on the Internet of Things, at 249 ll. 13-17, Nov. 19, 2013, *available at* http://www.ftc.gov/sites/default/files/documents/public_events/internet-things-privacy-security-connected-world/final_transcript.pdf; *id.* at 250 ll. 12-16.

[14] Yoshi Kohno, Transcript of FTC Workshop on the Internet of Things, at 242 ll. 6-15, Nov. 19, 2013, *available at* http://www.ftc.gov/sites/default/files/documents/public_events/internet-things-privacy-security-connected-world/final_transcript.pdf.

[15] *See* Timothy Hunter, Traffic Jams, Cell Phones, and Big Data, UC Berkeley AmpLab Blog, Jan. 18, 2012, *available at* https://amplab.cs.berkeley.edu/2012/01/18/traffic-jams-cell-phones-and-big-data/.

[16] *See* Doug Peeples, Is Big Data the Next Big Thing, SmartGridNews.com, Jan. 7, 2014, *available at* 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").

[17] *See, e.g.*, Brian Proffitt, *Big Data Analytics May Detect Infections Before Clinicians*, ITWORLD, Apr. 12, 2012, *available at* http://www.itworld.com/big-datahadoop/267396/big-data-analytics-may-detect-infection-clinicians.

[18] McKinsey & Co., Views from the Front Lines of the Big Data Analytics Revolution, Mar. 2014, *available at* 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).

decades, have manufactured "dumb" appliances and other devices take the steps necessary to keep secure the vast amounts of personal information that their newly smart devices will generate?

These are some of the big data privacy challenges presented by the Internet of Things that we all need to address.

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 sexual orientation, health conditions, religion, and race. A well-known, even infamous, example is Target's so-called "pregnancy prediction" score.[19] Using retail transaction data, Target was able to calculate, not only *whether* a consumer was pregnant, but also *when* her baby was due. It used the information to win the expectant mom's loyalty by offering coupons tailored to her stage of pregnancy.

And data brokers – entities that most folks know nothing about because they are not consumer-facing – are going far beyond this in the profiles that they develop from vast amounts of online and offline data.[20] A recent GAO report states that at least one data broker includes in its profiles about consumers information about 28 or more specific diseases, including cancer, diabetes, clinical depression, and prostate problems.[21] According to a Senate staff report released last December, 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.[22] And we recently read reports about another company that analyzes innocuous data from social media and the like to predict disease conditions like diabetes, obesity, and arthritis in order to persuade particular consumers to join medical trials. All of this creation, collection and use of health information is happening outside of HIPAA – outside any regulatory scheme to protect this information.

It's not hard to imagine the devices that I mentioned earlier, or their close cousins, feeding data into this system. Location, lifestyle, and all kinds of consumption habits could easily become available to data brokers and other analysts. Their inferences could soon be enriched by hard data from smart devices – before consumers even know that their devices are connected to the Internet.

---

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

[20] *See* CBS News, 60 Minutes, The Data Brokers: Selling Your Personal Information, Mar. 9, 2014, transcript available at http://www.cbsnews.com/news/the-data-brokers-selling-your-personal-information/.

[21] Gov't Accountability Office, *Information Resellers: Consumer Privacy Framework Needs to Reflect Changes in Technology and the Marketplace*, at 52, GAO-13-663, Sept. 2013, *available at* http://www.gao.gov/assets/660/658151.pdf (summarizing elements of Experian marketing lists).

[22] Senate Commerce Committee, *A Review of the Data Broker Industry: Collection, Use, and Sale of Consumer Data for Marketing Purposes* 12, Dec. 2013 (staff report), *available at* http://www.commerce.senate.gov/public/?a=Files.Serve&File_id=0d2b3642-6221-4888-a631-08f2f255b577 (citing documentary submission from Equifax); *id.* at 14 (listing health care-related data elements that Equifax maintains).

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 if data is inaccurate, misused, or through a security breach falls into the wrong hands. And we will pay a price in a lost sense of autonomy in a society in which information about some of the most sensitive aspects of our lives is available for analysts to examine without our knowledge or consent, and for anyone to buy if they are willing to pay the going price.

Second, we should all be concerned that questions about privacy will keep consumers away from the Internet of Things because they do not trust it. 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.[23] During our ongoing national discussion about NSA 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. But, as we've seen 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.

I believe that unchecked vacuuming of our information is not inevitable, that we can and should place some limits on untethered collection and retention of personal information about consumers. But the Internet of Things and big data analytics have led some to call for a shift in the emphasis that basic privacy principles should receive. Proponents of "risk-based frameworks" call attention to the difficulty of refraining from collecting unnecessary data and providing consumers with meaningful notice and choice about data collection and use.[24] These advocates argue that companies should instead take on the burden of assessing which uses of personal data pose risks to individuals and developing appropriate safeguards.[25]

I'm very much in favor of encouraging companies to think deeply about privacy risks – but it's essential for consumers to be involved in decisions about data use. That's where transparency and control – adapted for the data-intensive Internet of Things – come in.

Figuring out how to adapt our privacy framework and continue to encourage appropriate data minimization as well as adequate transparency and control mechanisms requires us to think about the roles that consumer-facing companies as well as non-consumer facing companies might play. Many of you work for, counsel, or consult with these companies. You have an excellent opportunity to make companies aware of the privacy risks they face and to steer them toward practical solutions – for consumers and the companies themselves. And you can't start too soon.

---

[23] *See, e.g.*, Christopher Wolf, Transcript of FTC Workshop on the Internet of Things, *supra* note 13, at 259 ll. 6-19.

[24] *See generally* Fred H. Cate, Peter Cullen, and Viktor Mayer-Schönberger, *Data Protection Principles for the 21st Century: Revising the OECD Guidelines*, Dec. 2013, *available at* http://www.oii.ox.ac.uk/publications/Data_Protection_Principles_for_the_21st_Century.pdf/

[25] *See id.* at 17.

Ensuring Transparency and Control on the Internet of Things: A Job for the Entire Industry

The Challenge for Device and Service Providers

The 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 grown and evolved in recent years. The best practices that the FTC described in its landmark 2012 Privacy Report would go a long way toward providing strong and appropriate consumer privacy protections with respect to the Internet of Things. I'd like to highlight three of these best practices.

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.[26] Privacy and ethical considerations are an increasingly hot topic among technologists in academia. As more and more schools provide their science and engineering students with this additional training, my guess is that smart companies will find better ways to put privacy and ethics considerations into practice.

Robust deidentification of personal data is another best practice that developers can use to protect 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.[27] 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 re-identify the data; and they should contractually prohibit downstream recipients from doing the same.[28] The technical prong of this framework poses challenges that researchers are continuing to tackle, with an eye toward the Internet of Things and beyond.[29]

And third, connected device developers should recognize that effective transparency is a fundamental building block of consumer privacy protections. The Commission recommends transparency improvements, including shorter, clearer, and more standardized notices and machine-readable notices, which could make it easier for consumers to

---

[26] *See* FED. TRADE COMM'N, PROTECTING CONSUMER PRIVACY IN AN ERA OF RAPID CHANGE: RECOMMENDATIONS FOR BUSINESSES AND POLICYMAKERS 22, Mar. 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 [FTC, 2012 PRIVACY REPORT].

[27] *See id.* at 21.

[28] *See id.*

[29] *See* MIT and White House Office of Science and Technology, 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.

understand what data their new devices collect and transmit.[30] Others are suggesting entirely new ways of providing notice, such as through "visual, auditory or tactile cues" tailored for a specific device.[31] And comprehensive, immersive apps or portals could help consumers gain a comprehensive view of how their devices are collecting and disclosing data.[32]

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 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.

Legislation, such as Chairman Rockefeller's and Senator Markey's Data Broker Accountability and Transparency Act,[33] would help. 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".[34] 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.

Here's how it would work. 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; 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 – relating to health conditions, sexual orientation, and financial condition, for example – the data brokers would provide greater transparency and more robust notice and choice to consumers.

The user interface is also critical. It should be user-friendly, and industry should provide a one-stop shop so consumers can learn about the tools all data brokers provide, and the choices consumers can make about the use of their data.

---

[30] FTC, 2012 PRIVACY REPORT, at 61-64.

[31] Future of Privacy Forum, Comment on Connected Smart Technologies in Advance of the FTC "Internet of Things" Workshop, at 6, May 31, 2013, *available at* http://www.ftc.gov/policy/public-comments/comment-00013-2.

[32] *See id.*

[33] Data Broker Accountability and Transparency Act of 2014 (DATA Act) (S. 2025), Feb. 12, 2014, *available at* http://beta.congress.gov/113/bills/s2025/BILLS-113s2025is.xml.

[34] *See generally* Julie Brill, *A Call to Arms: The Role of Technologists in Protecting Privacy in the Age of Big Data*, Sloan Cyber Security Lecture, Polytechnic Institute of NYU, Oct. 2013, *available at* http://www.ftc.gov/sites/default/files/documents/public_statements/call-arms-role-technologists-protecting-privacy-age-big-data/131023nyupolysloanlecture.pdf.

*****

Solving these privacy challenges is critical to ensuring that privacy is woven into the fabric of the Internet of Things. 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.