epic.org | ELECTRONIC PRIVACY INFORMATION CENTER

COMMENTS OF THE ELECTRONIC PRIVACY INFORMATION CENTER

to

NATIONAL TELECOMMUNICATIONS AND INFORMATION ADMINISTRATION,
U.S. DEPARTMENT OF COMMERCE

On the Benefits, Challenges, and Potential Roles for the Government in Fostering the Advancement of the Internet of Things

[Docket No. 160331306-6306-01]

June 2, 2016

By notice published on April 6, 2016, the National Telecommunications and Information Administration, U.S. Department of Commerce ("NTIA") seeks comments on the benefits, challenges, and potential roles for the U.S. government in fostering the advancement of the Internet of Things.[1] Pursuant to this notice, the Electronic Privacy Information Center ("EPIC") submits these comments and recommendations to urge NTIA to adequately protect the privacy of consumers who interact with the Internet of Things.

Specifically, EPIC recommends that legal requirements ensure that companies providing "Internet of Things" services adopt Privacy Enhancing Technologies; do not track, profile, or monitor users; minimize data collection; and ensure security in both design and operation of Internet-connected devices.

[1] Notice, Request for Public Comment, 81 Fed. Reg. 19,956 (Apr. 6, 2016).

EPIC is a public interest research center located in Washington, D.C. that focuses on emerging privacy and civil liberties issues and is a leading advocate for consumer privacy protections in the Internet of Things. EPIC has worked extensively on the privacy and security implications of this emerging field.[2] EPIC recently testified before the U.S. House of Representatives on the privacy and security implications of connected cars.[3]

I. PRIVACY RISKS OF THE INTERNET OF THINGS

Protecting consumer privacy will become increasingly difficult as the Internet of Things becomes increasingly prevalent. The ubiquity of connected devices enables collection of data about sensitive behavior patterns, which could be used in unauthorized ways or by unauthorized individuals. Edith Ramirez, chairwoman of the Federal Trade Commission ("FTC"), recently identified three key challenges that the Internet of Things poses to consumer privacy: "(1) ubiquitous data collection; (2) the potential for unexpected uses of consumer data that could have adverse consequences; and (3) heightened security risks."[4]

---

[2] *See, e.g.*, EPIC, *Internet of Things (IoT)*, https://epic.org/privacy/internet/iot/; EPIC Comments to the FTC, *On the Privacy and Security Implications of the Internet of Things* (June 1, 2013), https://epic.org/privacy/ftc/EPIC-FTC-IoT-Cmts.pdf.

[3] Khaliah Barnes, Testimony Before the U.S. House of Representatives Committee on Oversight and Government Reform, Subcommittees on Information Technology and Transportation and Public Assets, *The Internet of Cars* (Nov. 18, 2015), https://epic.org/privacy/edrs/EPIC-Connected-Cars-Testimony-Nov-18-2015.pdf. *See also*, EPIC et al., Comments to NHTSA, *Federal Motor Vehicle Safety Standards, Event Data Recorders* (Feb. 11, 2013), https://epic.org/privacy/edrs/EPIC-Coal-NHTSA-EDR-Cmts.pdf; EPIC Comments to NHTSA, *Federal Motor Vehicle Safety Standards: "Vehicle-to-Vehicle (V2V) Communications"* (Oct. 20, 2014), https://epic.org/privacy/edrs/EPIC-NHTSA-V2V-Cmts.pdf; Marc Rotenberg, *Are Vehicle Black Boxes a Good Idea?*, THE COSTO CONNECTION (Apr. 2013), http://www.costcoconnection.com/connection/201304?pg=24#pg24; Marc Rotenberg, *Steer Clear of Cars That Spy*, USA TODAY (Aug. 18, 2011), http://usatoday30.usatoday.com/news/opinion/editorials/2011-08-18-car-insurance-monitors-driving-snapshot_n.htm.

[4] Statement of FTC Chairwoman Edith Ramirez, *Privacy and the IoT: Navigating Policy Issues* (Jan 6, 2015), https://www.ftc.gov/system/files/documents/public_statements/617191/150106cesspeech.pdf?version=meter+at+0&module=meter-Links&pgtype=article&contentId=&mediaId=&referrer=&priority=true&action=click&contentCollection=meter-links-click.

Frank Pasquale, law professor and EPIC Advisory Board member, has warned of the impact of the Internet of Things on the workplace, cautioning that "the workplace plugged into the Internet of Things will be more productive and more prison-like (or, to be more accurate, more like an 'ankle monitor' of the mind that upgrades scanning not merely to location, but also to observable 'outputs' like typing and eye movements)."[5] Pasquale has also stated that while consumers may anticipate tracking of their Internet usage, "now with the Internet of Things, even our real space beyond the Internet is being monitored as well."[6]

Additionally, many Internet of Things devices feature "always on" tracking technology that surreptitiously records consumers' private conversations in their homes.[7] These "always on" devices raise numerous privacy concerns, including whether consumers have granted informed consent to this form of tracking. Moreover, even if the owner of an "always on" device has consented to constant, surreptitious tracking, a visitor to their home may not.

A. Data Collected from the Internet of Things May Reveal Sensitive Behavior Patterns That Consumers Wish to Keep Private

One of the primary risks internet users face as the Internet of Things expands is that the ubiquitous collection and storage of data about users can reveal sensitive behavior patterns. Smart Grid technology is a particularly illustrative example of this phenomenon.[8] A "Smart Grid" is an electrical or power grid that is equipped with telecommunications and Internet technologies used specifically to track user behavior in order to increase efficiency,

---

[5] Pew Research Center, *The Internet of Things Will Thrive by 2025* (May 14, 2014), http://www.pewinternet.org/files/2014/05/PIP_Internet-of-things_0514142.pdf.
[6] Frank Pasquale, *How Big Data's Inaccuracy Hurts People*, TRUE (2015), http://fleishmanhillard.com/2014/11/true/big-datas-inaccuracy-hurts-people/.
[7] EPIC Letter to DOJ Attorney General Loretta Lynch, FTC Chairwoman Edith Ramirez on "Always On" Devices (July 10, 2015), https://epic.org/privacy/internet/ftc/EPIC-Letter-FTC-AG-Always-On.pdf.
[8] EPIC Comments to NIST, *NIST Framework and Roadmap for Smart Grid Interoperability Standards Release 1.0* 4, (Nov. 9, 2009), https://epic.org/privacy/smartgrid/EPIC%20Smart%20Grid%20Comments.pdf.

sustainability, and economy.[9] Thus, a region's Smart Grid could track in real-time the actual amount of power used by particular buildings, streets, or homes, and could adjust its supply so that consumers are only provided with the amount of power they typically use at that point in the day or week.[10] However, a Smart Grid's capability to closely track consumer behavior poses a serious privacy risk. Information about consumers' power usage schedules can reveal intimate, personal details about their lives, such as their medical needs, interactions with others, and personal habits.[11] That concern is further exacerbated by the fact that Smart Grid meter data may track the usage of specific appliances within a person's home. Thus, a consumer's household activities could be determined as well, for instance whether the consumer uses medical equipment at night or the consumer's personal hygiene habits.[12]

B. Data Collected from the Internet of Things Could Be Used for Secondary Purposes Without Consumer Consent

The vast quantity of data generated by the Internet of Things creates the risk that this data could be used for purposes that are either unnecessary to the provision of a given service or not initially disclosed to the consumer. Smart devices could reveal a wealth of information about consumers' location, media consumption, activity patterns, associations, lifestyle, age, income, gender, race, and health – information with potential commercial value. Companies might attempt to exploit this data by using it to target advertising or selling it directly.[13] Because the Internet of Things generates data from all aspects of consumers' lives, these types of secondary uses could lead to the commercialization of intimate segments of consumers' lives.

---

[9] ARTICLE 29 DATA PROTECTION WORKING PARTY, OPINION ON THE DATA PROTECTION IMPACT ASSESSMENT TEMPLATE FOR SMART GRID AND SMART METERING SYSTEMS PREPARED BY EXPERT GROUP 2 OF THE COMMISSION'S SMART GRID TASK FORCE (2013).
[10] *Id*.
[11] EPIC Comments to NIST, *supra* note 8, at 4-5.
[12] *Id*. at 5.
[13] *Id.* at 8.

C. The Internet of Things has the Potential to Increase the Power Imbalance Between Consumers and Companies

In addition to the perceived invasiveness of smart devices and the sensitivity of the data they collect, the Internet of Things has the potential to exacerbate the power imbalance between consumers and the companies with which they conduct business. In most circumstances, the business-consumer relationship is already relatively one-sided. For many important services, such as utilities, telecommunications, and online services, consumers choose from a limited number of companies, which then present consumers with long form contracts, the terms of which are dictated and may be changed at will by the companies. These "take it or leave it" arrangements dominate the market for many important services, and they leave consumers relatively disempowered and without meaningful choice.[14]

The Internet of Things increases the relative power of companies by providing them with more information about consumers. Information is power, and smart devices will provide much more granular data about consumers' behavior to companies than has been traditionally available. Although some of this information might be available to consumers, powerful institutions will be able to use it more effectively.[15]

This concentration of power has important implications for the security of consumers' personal data. EPIC Advisory Board member, technologist, and security expert Bruce Schneier

[14] FED. TRADE COMM'N, PROTECTING CONSUMER PRIVACY IN AN ERA OF RAPID CHANGE 51 (2012), http://www.ftc.gov/os/2012/03/120326privacyreport.pdf.

[15] Bruce Schneier, *Will Giving the Internet Eyes and Ears Mean the End of Privacy?*, THE GUARDIAN (May 16, 2013), http://www.guardian.co.uk/technology/2013/may/16/internet-of-things-privacy-google ("These analytical limitations also mean that companies like Google and Facebook will benefit more from the Internet of Things than individuals – not only because they have access to more data, but also because they have more sophisticated query technology. And as technology continues to improve, the ability to automatically analyse this massive data stream will improve."); Bruce Schneier, *Power and the Internet*, SCHNEIER ON SECURITY (Jan. 31, 2013), https://www.schneier.com/blog/archives/2013/01/power_and_the_i.html ("The Internet empowers everyone. Powerful institutions might be slow to make use of that new power, but since they are powerful, they can use it more effectively."); *See generally*, Daniel Solove, *Privacy and Power: Computer Databases and Metaphors for Information Privacy* 53 STANFORD LAW REVIEW 1393 (2001).

has described the "feudal model" of security resulting from the removal of control from consumers, leaving them dependent on the practices of their service providers: "We give companies our data and trust them with our security, but we receive very few assurances of protection in return, and those companies have very few restrictions on what they can do."[16] This type of feudalism is driven by many factors, but one of the main developments Schneier cites is "Internet-enabled devices where the vendor maintains more control over the hardware and software than we do"—in other words, connected, smart devices like those constituting the Internet of Things.

These surveillance-enabled increases in power will also facilitate companies' ability to influence or direct the behavior of consumers.[17] This influence or direction may take many forms, and may be accomplished through a variety of consumer devices. For example, GPS and other networked technologies enable rental car companies to charge numerous "gotcha fees" for driving outside of specified regions or using certain services.[18]

II. CYBERSECURITY RISKS OF THE INTERNET OF THINGS

A significant risk to consumers in the Internet of Things is security, of both the users' data and their physical person. Many of the same security risks that currently threaten our data will only expand in the Internet of Things. The damage caused by malware, phishing, spam, and

[16] Bruce Schneier, *When It Comes to Security, We're Back to Feudalism*, WIRED, (Nov. 26, 2012), http://www.wired.com/opinion/2012/11/feudal-security/.
[17] Neil M. Richards, *The Dangers of Surveillance*, 126 HARV. L. REV. 1934 (2013) ("And while surveillance can sometimes have benign purposes (like traffic safety or parents using baby monitors or GPS trackers to monitor their children), it is invariably tied to a particular purpose. Critically, this purpose affects the power dynamic between the watcher and the watched, giving the watcher greater power to influence or direct the subject of surveillance").
[18] *Buck the Trend of Car Rental Surprise*, CONSUMER REPORTS (June 2011), https://www.consumerreports.org/cro/magazine-archive/2011/june/money/rental-car-surprises/car-rental/index.htm.

viruses will have an increasingly large array of networks in which to spread.[19] Additionally, not all wireless connections in the Internet of Things are encrypted.[20] Researchers who studied encryption within the Internet of Things found that "many of the devices exchanged personal or private information with servers on the Internet *in the clear*, completely unencrypted."[21]

In addition to data security risks, the Internet of Things also poses risks to physical safety and personal property. This is particularly true given that the constant flow of data so easily delineates sensitive behavior patterns, and flows over networks that are not always secure, leaving consumers vulnerable to malicious hackers.[22] For instance, a hacker could monitor Smart Grid power usage to determine when a consumer is at work, facilitating burglary, unauthorized entry, or worse.

A recent analysis of Smart Home security reveals additional safety risks posed by the Internet of Things. Researchers were able to remotely unlock front doors and set off fire alarms via Samsung's SmartThings platform.[23] Researchers have also found baby monitors vulnerable to hacking,[24] smart-watch motion sensors that can leak information on what wearers are typing,[25]

---

[19] *See* EUROPEAN COMM'N, A DIGITAL AGENDA FOR EUROPE, 16-18 (2010), http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2010:0245:FIN:EN:PDF

[20] Federal Motor Vehicle Safety Standards; Event Data Recorders, Docket No. NHTSA-2012-0177 (Comments of Privacy Coalition), 10 https://epic.org/privacy/edrs/EPIC-Coal-NHTSA-EDR-Cmts.pdf.

[21] Nick Feamster, *Who Will Secure the Internet of Things?*, FREEDOM TO TINKER (Jan. 19, 2016) https://freedom-to-tinker.com/blog/feamster/who-will-secure-the-internet-of-things/ (emphasis in original).

[22] M. Granger Morgan, et. al, *The Many Meanings of "Smart Grid,"* 5 (2009), http://www.epp.cmu.edu/Publications/Policy_Brief_Smart_Grid_July_09.pdf.

[23] Andy Greenberg, *Flaws in Samsung's 'Smart' Home Let Hackers Unlock Doors and Set Off Fire Alarms*, WIRED (May 2, 2016), https://www.wired.com/2016/05/flaws-samsungs-smart-home-let-hackers-unlock-doors-set-off-fire-alarms/.

[24] Dan Goodin, *9 Baby Monitors Wide Open to Hacks That Expose Users' Most Private Moments*, ARS TECHNICA (Sep. 2, 2015), http://arstechnica.com/security/2015/09/9-baby-monitors-wide-open-to-hacks-that-expose-users-most-private-moments/;

[25] Jennifer Abel, *Your Smartwatch Motion Sensors Could Tell Hackers What You're Typing*, CONSUMER AFFAIRS (Sep. 11, 2015), https://www.consumeraffairs.com/news/your-smartwatch-motion-sensors-could-tell-hackers-what-youre-typing-091115.html.

drug infusion pumps that allow hackers to raise medication dosages to fatal levels,[26] and pacemakers than can send deadly electric shocks through hacked transmitters.[27] Connected cars, also pose grave security threats that can place drivers and their families at serious risk of physical injuries and privacy harms.

III. THE INTERNET OF CARS POSES SIGNIFICANT PRIVACY AND CYBERSECURITY RISKS

Connected cars make up a significant segment of the Internet of Things, with new vehicles incorporating on-board navigation and tire pressure monitoring. But they also raise substantial privacy and safety concerns that should be addressed through meaningful, legally enforceable safeguards.

A. Connected Cars Collect and Broadcast Troves of Sensitive Personal Data

Modern cars contain dozens of small computers, known as electronic control units, which are linked together by the car's internal computer network.[28] These computers control everything from braking, acceleration, steering, engine performance, door locks, and climate control to navigation and entertainment.[29] These systems can also "record vehicle data to analyze and improve performance."[30]

---

[26] Kim Zetter, *Hacker Can Send Fatal Dose to Hospital Drug Pumps*, WIRED (June 8, 2015), https://www.wired.com/2015/06/hackers-can-send-fatal-doses-hospital-drug-pumps/.
[27] Darren Pauli, *Hacked Terminals Capable of Causing Pacemaker Deaths*, ITNEWS (Oct. 17, 2012), http://www.itnews.com.au/news/hacked-terminals-capable-of-causing-pacemaker-mass-murder-319508.
[28] *See Tracking & Hacking: Security & Privacy Gaps Put American Drivers at Risk*, Sen. Edward J. Markey (D-Mass) (Feb. 2015), https://www.markey.senate.gov/imo/media/doc/2015-02-06_MarkeyReport-Tracking_Hacking_CarSecurity%202.pdf [hereinafter "Markey Report"]; David Gelles, Hiroko Tabuchi & Matthew Dolan, *Complex Car Software Becomes the Weak Spot Under the Hood*, N.Y. TIMES (Sep. 26, 2015), http://www.nytimes.com/2015/09/27/business/complex-car-software-becomes-the-weak-spot-under-the-hood.html?_r=0; Andy Greenberg, *Hackers Remotely Kill a Jeep on the Highway – With Me in It*, WIRED (July 21, 2015), https://www.wired.com/2015/07/hackers-remotely-kill-jeep-highway/.
[29] *See* Gelles, Tabuchi & Dolan, *supra* note 28; Greenberg, *supra* note 28.
[30] Markey Report at 3.

As cars become more technologically sophisticated, they acquire the ability to collect and disclose huge amounts of sensitive driving data. According to a U.S. Senate report, nearly a third of all of cars from 13 major manufacturers implement technologies that collect driving history information.[31] These technologies include "navigation, telematics, infotainment, emergency assist, stolen vehicle recovery, and event data recording systems."[32]

Many modern cars contain "telematics" systems, which "use telecommunication networks and GPS signals to allow information, such as location data, to be communicated between a car and a service provider."[33] According to 2014 Government Accountability Office testimony, the collection and sharing of consumer location information by in-car navigation providers pose serious risks to consumer privacy.[34] Storing location information over time "create[s] a detailed profile of individual behavior, including habits, preferences, and routes traveled," the exploitation of which can lead to identity theft or threats to personal safety.[35] In particular, the GAO report noted that in-car navigation providers "use different de-identification methods that may lead to varying levels of protection for consumers."[36]

B. Cybersecurity Weaknesses of Connected Cars Place Drivers at Serious Risk of Physical Injury and Privacy Harms

Nearly all cars on the road today include at least one wireless entry point ("WEP").[37] WEPs are essential to the functionality of built-in wireless features such as tire pressure monitoring systems, "Bluetooth, keyless entry, remote start, navigation, WiFi, cellular/telematics,

---

[31] *Id*. at 8.
[32] *Id*.
[33] U.S. Gov. Accountability Office, GAO-14-649T, *Consumers' Location Data: Companies Take Steps to Protect Privacy, but Practices Are Inconsistent, and Risks May Not be Clear to Consumers* (2014), http://gao.gov/products/GAO-14-649T.
[34] *Id*. at 2.
[35] *Id*.
[36] *Id*.
[37] Markey Report at 5.

radio, and anti-theft systems and features."[38] Unfortunately, WEPs also provide entry points for remote vehicle hacking. A 2011 report by computer scientists showed how a hacker could use WEPs to "take control of various features — like the car locks and brakes — as well as to track the vehicle's location, eavesdrop on its cabin and steal vehicle data."[39]

In a 2013 study, researchers Charlie Miller and Chris Valasek connected laptops to the computer systems of a Toyota Prius and a Ford Escape and were able to jerk the wheel at high speeds, turn the car, cause sudden acceleration or braking, turn on the horn, tighten the seatbelts in anticipation of a nonexistent crash, and kill the brakes.[40] In 2014, a researcher wirelessly killed a car's engine and disabled its brakes as it drove up a ramp.[41] Last year, Miller and Valasek remotely hacked a Jeep Cherokee traveling on a highway ten miles from their computers.[42] The pair were able to manipulate the air conditioning, turn on the radio, activate the windshield wipers and wiper fluid, take over the car's digital display screen, cut the transmission, kill the engine, and engage and disable the brakes.[43] In response to the reported hack, Fiat Chrysler recalled more than 1.4 million vehicles.[44]

---

[38] *Id*.
[39] John Markoff, *Researchers Show How a Car's Electronics Can Be Taken Over Remotely*, N.Y. Times (Mar. 9, 2011), http://www.nytimes.com/2011/03/10/business/10hack.html.
[40] Charlie Miller & Chris Valasek, *Adventures in Automotive Networks and Control Units*, IOActive (2014) http://www.ioactive.com/pdfs/IOActive_Adventures_in_Automotive_Networks_and_Control_Units.pdf; Steve Henn, *With Smarter Cars, The Doors Are Open To Hacking Dangers*, NPR (July 30, 2013), http://www.npr.org/sections/alltechconsidered/2013/07/30/206800198/Smarter-Cars-Open-New-Doors-To-Smarter-Thieves.
[41] Xavier Aaronson, *We Drove a Car While It Was Being Hacked*, MOTHERBOARD (May 29, 2014), http://motherboard.vice.com/read/we-drove-a-car-while-it-was-being-hacked.
[42] Greenberg, *supra* note 28.
[43] *Id*.
[44] Alex Hern, *Fiat Chrysler Recalls 8,000 More Jeeps Over Wireless Hacking*, THE GUARDIAN (Sep. 7, 2015), https://www.theguardian.com/technology/2015/sep/07/fiat-chrysler-recalls-more-jeeps-wireless-hacking.

So far, researchers and scientists in controlled settings have done most of the reported hacks of moving cars.[45] But wide-scale malicious automobile hacking is certainly imminent, if not already occurring. Thieves can already hack computer-based door lock systems to rob parked cars.[46] And in 2010, a disgruntled former car salesman disabled more than one hundred cars in Austin, Texas by hacking into a "web-based vehicle-immobilization system normally used to get the attention of consumers delinquent in their auto payments."[47]

The very real possibility of remote car hacking poses substantial risks to driver safety and security. Cars can be remotely hacked and controlled from anywhere in the world via the Internet.[48] Wireless hacking can also give hackers access to the car's physical location using built-in GPS navigation systems, which would facilitate crimes such as harassment, stalking, and car theft.[49]

IV. RECOMMENDATIONS FOR ADDRESSING THE PRIVACY AND SECURITY RISKS OF THE INTERNET OF THINGS

A. The Government Should Require Companies That Collect Data From Smart Devices to Implement Privacy Enhancing Technologies

EPIC has advocated for Privacy Enhancing Technologies ("PETs") to protect privacy.[50] PETs limit data collection and embed privacy protection.[51] Rather than building a connected car that is capable of storing potentially limitless travel records, for instance, a Privacy Enhancing

---

[45] *Id*.
[46] Nick Bilton, *Keeping Your Car Safe From Electronic Thieves*, N.Y. TIMES (Apr. 15, 2015), http://www.nytimes.com/2015/04/16/style/keeping-your-car-safe-from-electronic-thieves.html.
[47] Kevin Poulsen, *Hacker Disables More Than 100 Cars Remotely*, WIRED (Mar. 17, 2012), https://www.wired.com/2010/03/hacker-bricks-cars/.
[48] Greenberg, *supra* note 28.
[49] *Id*.
[50] Herbert Burkert, *Privacy-Enhancing Technologies: Typology, Critique, Vision* in TECHNOLOGY AND PRIVACY: THE NEW LANDSCAPE 125 (Philip E. Agre and Marc Rotenberg eds. 1998).
[51] Alec Foege, *IBM's Jeff Jonas on Baking Data Privacy into Predictive Analytics*, DATA INFORMED (Nov. 20, 2013) http://data-informed.com/ibms-jeff-jonas-baking-data-privacypredictiveanalytics/#sthash.hBM0lg1N.dpuf.

Technology would automatically delete old data after a certain amount of time, or prevent individual data from being automatically synced with a central database. There are several well-established methods of implementing PETs, and in the Internet of Things, all of these methods will be necessary.

B. The Government Must Protect Consumers' Rights to Limit Data Collection and Use

Individuals should retain control over their personal data, including the right to limit the collection and use of data beyond that necessary to the provision of the service. A "notice and choice" or consent-based approach to privacy protections simply does not work in the Internet of Things. As one commenter explains,

> Internet of Things devices generally have no screen or keyboard, and thus giving consumers data and privacy information and an opportunity to consent is particularly challenging. Current Internet of Things products often fail to notify consumers about how to find their relevant privacy policy, and once found, such policies are often confusing, incomplete, and misleading.[52]

Notice and choice is insufficient to protect consumer privacy in the traditional online ecosystem,[53] and will be even less effective in the Internet of Things. Moreover, privacy experts have observed that "user choice will frequently be illusory in a ubiquitously sensed environment."[54] Instead, Fair Information Practices must be fully applied to the Internet of Things.[55] This approach would grant consumers affirmative rights and place privacy responsibilities on companies who collect consumer data from connected devices.

---

[52] Scott R. Peppet, *Regulating the Internet of Things: First Steps Toward Managing Discrimination, Privacy, Security, and Consent*, 93 Tex. L. Rev. 85, 95 (2014).
[53] *See* Marc Rotenberg, *Fair Information Practices and the Architecture of Privacy*, 2001 STAN. TECH. L. REV. 1 (2001).
[54] Ellen P. Goodman, *The Atomic Age of Data: Policies for the Internet of Things* 24, THE ASPEN INSTITUTE COMMUNICATIONS AND SOCIETY PROGRAM (2015), http://csreports.aspeninstitute.org/documents/Atomic_Age_of_Data.pdf.
[55] *See* EPIC, *The Code of Fair Information Practices*, http://epic.org/privacy/consumer/code_fair_info.html.

Companies that collect data from smart devices must be required to provide access to this data for consumers. Many of the consumer benefits[56] of the Internet of Things—reduced costs, time savings, increased convenience—require or would be greatly improved by providing consumers with access to their data. Any data collected by smart devices should be made available to consumers through any laptop, tablet, or smartphone. Furthermore, consumers should also be able to access the basic logic behind any algorithm used by a company or vendor to make a decision about a consumer. For instance, if a Smart Grid central database determines that, based on their energy consumption, certain energy consumers will have their power switched off at certain times of the day, those consumers must be informed that their data classification has changed. Transparency is therefore a vital component of informed user choice.[57]

C. Companies Should Minimize Collection of Data Generated By Smart Devices

Companies should be required to adopt the principle of data minimization, so that only so much data is used and stored as is necessary to ensure the functionality of their products or services.[58] Minimization itself can be accomplished in a number of ways. Data could be collected periodically or randomly, rather than constantly; or companies could take data samples from a representative percentage of products, rather than collecting data from every product. Companies could collect only aggregated data to avoid obtaining granular information about particular consumers. For example, a Smart Grid could collect aggregate data from an entire apartment building, rather than collecting individual data from each apartment, or even from individual devices within each apartment. Aggregation combined with deletion – i.e., storing individual

[56] *See, e.g., 4 ways the internet of things will radically change your life*, WHITEBOARD http://www.whiteboardmag.com/4-ways-the-internet-of-things-will-radically-change-your-life/.
[57] *Id*.
[58] *Id*. at 23-24.

data only for as long as it takes to develop an aggregate computation – could allow for very accurate aggregation, while ensuring a degree of anonymity for the consumers. Data retention periods should be restricted as well.

V. CONCLUSION

The Internet of Things presents important implications for consumer privacy and security. The government must act now to ensure these technologies are implemented in a way that benefits consumers and respects important values. EPIC welcomes the opportunity to work with NTIA on this issue in the future.

Respectfully Submitted,

Marc Rotenberg,
EPIC President and Executive Director

Khaliah Barnes
EPIC Associate Director and Administrative Law Counsel

Claire Gartland
EPIC Consumer Protection Counsel