COMMENTS OF THE ELECTRONIC PRIVACY INFORMATION CENTER

to

THE FEDERAL TRADE COMMISSION

On the Privacy and Security Implications of the Internet of Things

"FTC File No. ___"

June 1, 2013

By notice published on April 17, 2013, the Federal Trade Commission ("FTC" or "Commission") seeks comments on the privacy and security implications of the Internet of Things.[1] Pursuant to this notice, the Electronic Privacy Information Center ("EPIC") submits these comments and recommendations to ensure that the final order adequately protects the privacy of consumers who interact with these Companies.

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 consumer advocate before the FTC. EPIC has a particular interest in protecting consumer privacy, and has played a leading role in developing the authority of the Commission to address emerging privacy issues and to safeguard the privacy rights of consumers.[2] EPIC's 2010 complaint concerning Google Buzz provided the basis for the Commission's investigation and October 24, 2011 subsequent settlement concerning

[1] Press Release, Fed. Trade Comm'n, FTC Seeks Input on Privacy and Security Implications of the Internet of Things (Apr. 17, 2013), http://www.ftc.gov/opa/2013/04/internetthings.shtm.

[2] *See, e.g.*, Letter from EPIC Executive Director Marc Rotenberg to FTC Commissioner Christine Varney, EPIC (Dec. 14, 1995) (urging the FTC to investigate the misuse of personal information by the direct marketing industry), http://epic.org/privacy/internet/ftc/ftc_letter.html; DoubleClick, Inc., *FTC* File No. 071-0170 (2000) (Complaint and Request for Injunction, Request for Investigation and for Other Relief), http://epic.org/privacy/internet/ftc/DCLK_complaint.pdf; Microsoft Corporation, FTC File No. 012 3240 (2002) (Complaint and Request for Injunction, Request for Investigation and for Other Relief), http://epic.org/privacy/consumer/MS_complaint.pdf; Choicepoint, Inc., FTC File No. 052-3069 (2004) (Request for Investigation and for Other Relief) , http://epic.org/privacy/choicepoint/fcraltr12.16.04.html.

the improper disclosure of user information.[3] In that case, the Commission found that Google "used deceptive tactics and violated its own privacy promises to consumers when it launched [Buzz]."[4] The Commission's settlement with Facebook also followed from a Complaint filed by EPIC and a coalition of privacy and civil liberties organization in December 2009 and a Supplemental Complaint filed by EPIC in February 2010.[5] EPIC has also submitted comments for and participated in numerous Commission workshops, such as Face Facts: A Forum on Facial Recognition Technology,[6] and In Short: Advertising and Privacy Disclosures in a Digital World.[7]

The Commission public comment on the privacy and security implications of the growing capacity of Internet-connected devices to communicate with one another, sometimes described as "The Internet of Things."[8] The Commission asks about "the significant developments in services and products that make use of this connectivity"; "the various technologies that enable this connectivity"; "the unique privacy and security concerns associated with smart technology and its data"; and techniques, such as security patching and de-identification, for reducing these privacy and security concerns.[9]

In the comments below, EPIC describes several of the most common consumer devices and the technologies that enable their connectivity. A host of communicative technologies could

[3] Press Release, Federal Trade Comm'n, FTC Charges Deceptive Privacy Practices in Google's Rollout of Its Buzz Social Network (Mar. 30, 2011), http://ftc.gov/opa/2011/03/google.shtm ("Google's data practices in connection with its launch of Google Buzz were the subject of a complaint filed with the FTC by the Electronic Privacy Information Center shortly after the service was launched.").
[4] *Id.*
[5] Facebook, Inc., (2009) (EPIC Complaint, Request for Investigation, Injunction, and Other Relief), https://epic.org/privacy/inrefacebook/EPIC-FacebookComplaint.pdf; Facebook, Inc., (2010) (EPIC Supplemental Materials in Support of Pending Complaint and Request for Injunction, Request for Investigation and for Other Relief); Facebook, Inc., (2010) (EPIC Complaint, Request for Investigation, Injunction, and Other Relief) , https://epic.org/privacy/facebook/EPIC_FTC_FB_Complaint.pdf.
[6] Face Facts: A Forum on Facial Recognition Technology, FED. TRADE COMM'N, http://www.ftc.gov/bcp/workshops/facefacts/ (last visited May 31, 2013)
[7] In Short: Advertising and Privacy Disclosures in a Digital World, FED. TRADE COMM'N, http://www.ftc.gov/bcp/workshops/inshort/ (last visited May 31, 2013)
[8] Fed. Trade Comm'n, *supra* note 1.
[9] *Id.*

enable the Internet of Things, including IPv6, RFID, Wi-Fi, and GPS, and these technologies could be used in a wide variety of devices, from household appliances to smartphones to wearable computers. EPIC also outlines the main privacy and security concerns associated with these devices. For example, the ubiquity of connected devices would enable to collection of data about sensitive behavior patterns, which could be used in unauthorized ways or by unauthorized individuals. Finally, EPIC makes several recommendations for reducing these privacy and security concerns. Specifically, EPIC recommends that the Commission enforce Fair Information Practices, require companies to adopt Privacy Enhancing Techniques, respect a consumer's choice not to tracked, profiled, or monitored, minimize data collection, and ensure transparency in both design and operation of Internet-connected devices.

I. Technologies and Devices of the Internet of Things

A. Wireless Radio Technologies: Wi-Fi, Bluetooth, RFID, and NFC

The radio frequency portion of the electromagnetic spectrum[10] facilitates many communications technologies that enable the Internet of Things. Wi-Fi, Bluetooth, Radio-Frequency Identification ("RFID") and Near-Field Communication ("NFC") technologies both use radio waves to enable tracking and communication between objects and devices.

Wi-Fi networks operate through an access point (or "router") and one or more Wi-Fi connected devices. Home Wi-Fi networks transmit signals in two FCC-unlicensed frequency

[10] The electromagnetic spectrum is "the full range of frequencies, from radio waves to gamma rays, that characterizes light." *Imagine the Universe! Dictionary*, NASA, http://imagine.gsfc.nasa.gov/docs/dict_ei.html#em_waves (last visited May 31, 2013). Radio waves, the form of electromagnetic radiation with the lowest energy, occupy of the portion of the electromagnetic spectrum with frequencies between .01 Megahertz (MHz) and 300,000 MHz. *NRAO Radio Astronomy Glossary*, NAT'L RADIO ASTRONOMY OBSERVATORY, http://www.nrao.edu/imagegallery/glossary.shtml#r (last visited May 31, 2013). In the United States, the Federal Communications Commission (FCC) and the National Telecommunications and Information Administration (NTIA) allocate the radio spectrum frequencies between .009 MHz and 275,000 MHz. *Radio Spectrum Allocation*, FED. COMMC'N COMM'N, http://www.fcc.gov/encyclopedia/radio-spectrum-allocation (last visited May 31, 2013).

bands: 2400 MHz and 5000 MHz.[11] Whether a Wireless Local Area Networks ("WLAN") device broadcasts in the 2400 MHz band, the 5000 MHz band, or both, depends upon which of the Institute of Electrical and Electronics Engineers' (IEEE) 802.11 operating standards the device follows.[12] The most recent amendment, 802.11n, allows for operation alternatively or concurrently in both the 2400 and 5000 MHz bands.[13] Although the FCC does not require a license to broadcast at 2400 and 5000 MHz, the agency does limit the peak output power of such devices to 1 watt.[14] Other standards have been designed to provide Wi-Fi communication among devices within a broad geographic range. Worldwide Interoperability for Microwave Access (WiMAX) and the 802.16 Wireless Metropolitan Network ("WMAN") standard upon which WiMAX is based are both designed to broadcast over a range of several miles.[15] And the 802.11p standard has been developed to facilitate intelligent transportation systems.[16]

[11] *See* 47 C.F.R. §§ 15.247, 15.401-407; *see also* FED. COMMC'N COMM'N, SPECTRUM POLICY TASK FORCE, REPORT OF THE UNLICENSED DEVICES AND EXPERIMENTAL LICENSES WORKING GROUP 8, 10 (2002) *available at* http://transition.fcc.gov/sptf/files/E&UWGFinalReport.pdf. (listing the unlicensed frequency ranges as 902-928 MHz, 2400-2483.5 MHz, 5150-5350 MHz, and 5725-5850 MHz)

[12] The 802.11 series includes the general-purpose Wi-Fi 802.11a, 802.11b, 802.11g, and 802.11n standards, each of which differs slightly in bandwidth and signal frequency. *See IEEE 802.11: Wireless Local Area Networks (LANs)*, IEEE Standards Ass'n, http://standards.ieee.org/about/get/802/802.11.html (last visited May 31, 2013). The 802.11a standard operates in the 5000 MHz band, the 802.11b and 802.11g standards operate in the 2400 MHz band, and the 802.11n standard has the capability of operating alternatively or concurrently in the 2400 and 5000 MHz bands.

[13] *See* IEEE COMPUTER SOC'Y, IEEE STANDARD FOR INFORMATION TECHNOLOGY-TELECOMMUNICATIONS AND INFORMATION EXCHANGE BETWEEN SYSTEMS-LOCAL AND METROPOLITAN AREA NETWORKS-SPECIFIC REQUIREMENTS: PART 11: WIRELESS LAN MEDIUM ACCESS CONTROL (MAC) AND PHYSICAL LAYER (PHY) SPECIFICATIONS – AMENDMENT 5: ENHANCEMENTS FOR HIGHER THROUGHPUT (2009), http://standards.ieee.org/getieee802/download/802.11n-2009.pdf.

[14] *See* 47 C.F.R. § 15.247(b).

[15] *See Resources – Frequently Asked Questions*, WIMAX FORUM, http://www.wimaxforum.org/resources/frequently-asked-questions ; *IEEE 802.16: Broadband Wireless Metropolitan Area Networks (MANs)*, IEEE STANDARDS ASS'N, http://standards.ieee.org/about/get/802/802.16.html.

[16] *See* IEEE COMPUTER SOC'Y, IEEE STANDARD FOR INFORMATION TECHNOLOGY-- LOCAL AND METROPOLITAN AREA NETWORKS-- SPECIFIC REQUIREMENTS-- PART 11: WIRELESS LAN MEDIUM ACCESS CONTROL (MAC) AND PHYSICAL LAYER (PHY) SPECIFICATIONS AMENDMENT 6: WIRELESS ACCESS IN VEHICULAR ENVIRONMENTS (2010), http://standards.ieee.org/findstds/standard/802.11p-2010.html.

Bluetooth technology uses small computer chips equipped with wireless antennas to communicate with other Bluetooth devices.[17] Bluetooth devices communicate in the unlicensed Industry, Industrial, Scientific and Medical ("ISM") 2.4 MHz frequency band.[18] Connected Bluetooth devices form a communications network, or piconet, consisting of a master device that defines the characteristics of the Bluetooth connection, and up to seven slave devices. Communication occurs hierarchically between the master and slave devices, and not directly between slave devices.[19] Range varies from 3-300 feet according to the class of radio used in a Bluetooth chip, with the most common class having a range of 33 feet.[20]

RFID communication operates through tags, which contain wireless antennas and small amounts of memory, and readers, which receive and decode data stored on RFID tags.[21] "Passive" RFID tags use the wireless signal from readers as a power source and can only transmit data when scanned, whereas "active" RFID tags contain their own power source and can transmit data over long distances.[22] RFID applications use a variety of standards and frequencies, depending on use.[23] The range of an RFID tag varies from under 3 feet to 300 feet according to several factors, including whether the tag is active or passive, with longest ranges coming from battery-powered RFID readers.[24]

---

[17] *Fast Facts*, BLUETOOTH SPECIAL INTEREST GROUP, http://www.bluetooth.com/Pages/Fast-Facts.aspx (last visited May 31, 2013).
[18] *Building with Technology*, BLUETOOTH SPECIAL INTEREST GROUP, https://www.bluetooth.org/en-us/test-qualification/product-development-overview/building-technology (last visited May 31, 2013).
[19] BLUETOOTH SPECIAL INTEREST GROUP, SPECIFICATION OF THE BLUETOOTH SYSTEM 157 (2010), *available at* https://www.bluetooth.org/en-us/specification/adopted-specifications (click "Core Version 4.0").
[20] BLUETOOTH SPECIAL INTEREST GROUP, *supra* note 18
[21] *Radio Frequency Identification (RFID) Systems*, EPIC, https://epic.org/privacy/rfid/ (last visited May 31, 2013).
[22] *See* Kevin Werbach, *Sensors and Sensibilities*, 28 Cardozo L. Rev. 2321, 2329-30 (2007); *What's the difference between passive and active tags?*, RFID Journal, http://www.rfidjournal.com/faq/show?68 (last visited May 31, 2013).
[23] Bob Violino, *A Summary of RFID Standards*, RFID JOURNAL (Jan. 16, 2005) http://www.rfidjournal.com/articles/view?1335/
[24] *From how far away can a typical RFID tag be read?*, RFID JOURNAL, http://www.rfidjournal.com/faq/show?139(last visited May 31, 2013).

NFC relies on magnetic induction to transmit data between devices.[25] NFC devices are similar to 13.56MHz RFID tags.[26] Like RFID, NFC operates in two communication modes: passive, where only one NFC device transmits data, and active, where both NFC devices transmit data.[27] But NFC operates over a much shorter range than any of the aforementioned radio communication technologies: 4 inches or less.[28]

These technologies enable communication in a wide variety of devices. Wi-Fi is currently used by laptops, smartphones, and tablets, and may be used by autonomous vehicles[29] and smart grid appliances.[30] RFID has been used for several years to track merchandise[31] and to enable electronic toll-collection systems, such as EZ Pass.[32] NFC will be used to facilitate mobile payments.[33] Wearable computers, such as Google Glass, will also likely be compatible with most or all communication standards.[34] Importantly, many wireless/RF devices contain unique identifiers, such as the International Mobile Station Equipment Identity ("IMEI") numbers on mobile phones and the 96-bit identification code on RFID tags.

---

[25] Dan Nosowitz, Everything You Need to Know About Near Field Communication, POPULAR SCIENCE (Mar. 1, 2011), http://www.popsci.com/gadgets/article/2011-02/near-field-communication-helping-your-smartphone-replace-your-wallet-2010/.

[26] *How Does NFC Technology Work?*, NFC FORUM, http://www.nfc-forum.org/resources/faqs#howwork (last visited May 31, 2013).

[27] INNOVISION RESEARCH AND TECHNOLOGY PLC, NEAR FIELD COMMUNICATION IN THE REAL WORLD 5, *available at* http://www.nfc-forum.org/resources/white_papers/Innovision_whitePaper1.pdf

[28] Nosowitz, *supra* note 25.

[29] Darlene Storm, *Privacy and the car of the future: Cars talking to each other and to infrastructure*, ComputerWorld (Jan. 3, 2013), http://blogs.computerworld.com/privacy/21571/privacy-and-car-future-cars-talking-each-other-and-infrastructure.

[30] *See* WI-FI ALLIANCE, WI-FI FOR THE SMART GRID: MATURE, INTEROPERABLE, SECURE TECHNOLOGY FOR ADVANCED SMART ENERGY MANAGEMENT COMMUNICATIONS (2010), *available at* http://www.wi-fi.org/knowledge-center/white-papers/wi-fi%C2%AE-smart-grid-mature-interoperable-secure-technology-advanced; NAT'L INST. OF STANDARDS AND TECH., NIST FRAMEWORK AND ROADMAP FOR SMART GRID INTEROPERABILITY STANDARDS, RELEASE 2.0 47 (2012), http://www.nist.gov/smartgrid/upload/NIST_Framework_Release_2-0_corr.pdf

[31] Werbach, *supra* note 22, at 2329-30.

[32] Claire Swedberg, *Efforts to Aid Adoption of ISO 18000-6C RFID for Toll Collection Move Forward*, RFID JOURNAL (Oct. 18, 2012), http://www.rfidjournal.com/articles/view?10038.

[33] Christina Warren, *Samsung and Visa Take NFC Mobile Payments Global*, MASHABLE (Feb. 25, 2013), http://mashable.com/2013/02/25/samsung-visa-nfc/

[34] *Google Glass Tech Specs*, GOOGLE, https://support.google.com/glass/answer/3064128?hl=en (last visited May 31, 2013).

B. Internet Communications Protocols: IPv6

Another technology that is poised to allow even more granular identification of individual internet-connected devices is IPv6. IPv6 is the most recent version of the protocol that is used to assign IP addresses.[35] IP addresses are the "housing addresses" of networked devices.[36] Generally, each device is assigned a unique number, which directs all packets of information going to and from the device.[37] Like a housing (or business) address, however, multiple devices frequently share the same IP address. This is possible through the use of routers, which assign separate, sub-addresses to individual devices in local networks.[38] For example, although the router in a small office network of 10 devices would assign a unique, local address to each device, once the data from the devices passes outside the local environment, all packets will appear to originate from just one IP address – the one assigned to the router. This feature of the current IP system means that individual devices that are part of a local network enjoy a certain degree of anonymity. While an inspection of the packets emerging from a particular IP address can reveal the kind of data traveling to or from the router, it is much harder to trace the activity to a particular device within a router's network.[39]

The most widely used IP code currently, IPv4, assigned thirty-two bit addresses.[40] This means that IPv4 had the capacity to assign approximately 4.3 billion unique IP addresses (2^{32}

[35] *See Search Engine Privacy*, EPIC, https://epic.org/privacy/search_engine/; SANGAM RACHERLA & JASON DANIEL, IBM, IPV6 INTRODUCTION AND CONFIGURATION 2 (2012), *available at* http://www.redbooks.ibm.com/redpapers/pdfs/redp4776.pdf.
[36] Christopher Parsons, IPv6 and the Future of Privacy (Mar. 9, 2010), http://www.christopher-parsons.com/ipv6-and-the-future-of-privacy.
[37] *Id.*
[38] Riva Richmond, We Know Where You Are, Wall Street J., Sep. 29, 2008, *available at* http://online.wsj.com/article/SB122227759888771725.html.
[39] *Id.*
[40] Bill Frezza, *Where's all the outrage about the IPv6 privacy threat?*, 783 INTERNETWEEK 43 (1999), *reprinted at* http://www.ipv6.ru/russian/presscenter/press/ebsco/1.php.

addresses).[41] However, the rapid increase in the number of internet connected devices that use IP addresses exhausted the limitations of IPv4, which ran out of unique addresses on February 3, 2011.[42] Of course, programmers had been anticipating IP address depletion since the 1980s, and new, networked devices were being regularly assigned IPv6 addresses by 2008.[43] IPv6 assigns 128-bit addresses, which means that it has the capacity to assign 2^{128}, or approximately 340 trillion trillion trillion addresses.[44] This means that there are now effectively limitless quantities of unique IP addresses available to identify new devices, in addition to the 4.3 billion IPv4 addresses already in existence.

The implications for IPv6 in the Internet of Things lie in the fact that, without the need for local networks in order to share IP addresses, every device that connects to the internet can have its own, unique, persistent identifier. Early IPv6 implementations used an addressing scheme that tied a user's IPv6 address to the embedded network hardware access address. This mechanism would have the effect of creating an unchangeable, unique identifier that could be used to correlate unrelated activity and to allow a user to be tracked across multiple networks.[45] To address this privacy and security threat, the Internet Engineering Task Force developed RFC 3041, "Privacy Extensions for Stateless Autoconfiguration in IPv6," which enables users to periodically randomize their IPv6 address as well as to generate temporary addresses, thus preventing the creation of a unique, unchangeable IPv6 address assigned to a specific person.[46] Similarly, the Article 29 Working Party's Opinion on IPv6 recommends that "network and

[41] *Id.*
[42] Number Resource Organization, Free Pool of IPv4 Address Space Depleted, Feb. 3, 2011, available at http://www.nro.net/news/ipv4-free-pool-depleted.
[43] *Parsons*, supra at 2.
[44] Racherla & Daniel at 10.
[45] See Comments of EPIC, Request for Comments on Deployment of Internet Protocol, Version 6, NTIA Docket No. 040107006-4006-01, *available at* https://epic.org/privacy/internet/IPv6_comments.pdf
[46] *See id.*

access providers should offer to any user the option to use the network or to access the services anonymously or using a pseudonym."[47]

C. Satellite: Global Positioning Systems

The Global Positioning System ("GPS") is a satellite-based service that enables individuals to determine their precise location anywhere on Earth. The U.S. government operates GPS, and provides free access to the public.[48] Anyone can use an electronic device, commonly called a "GPS receiver," to access GPS signals and determine their precise location, altitude, and speed.[49] GPS relies on a minimum of 24 satellites configured to provide navigation and timing information worldwide on a constant 24 hour per day basis.[50] There are currently 31 satellites, including "back-up" satellites, in the GPS constellation.[51] GPS satellites can provide three-dimensional location data (longitude, latitude and altitude) as well as precise velocity and timing information to an unlimited number of users simultaneously.[52] GPS signals "are so accurate, time can be figured to within a millionth of a second, velocity within a fraction of a mile per hour and location to within 100 feet."[53]

A GPS receiver calculates and typically displays its location, velocity, altitude, and the time by decoding data from the GPS satellite network.[54] This means that as the receiver moves, it continuously updates its location. Furthermore, GPS receivers are small enough and accurate

[47] Article 29 Data Protection Working Party, Opinion 2/2002 on the use of unique identifiers in telecommunication terminal equipments: the example of IPv6, at 3 (2002), http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2002/wp58_en.pdf
[48] 10 U.S.C. § 2281(b) (2011).
[49] ANITA L. ALLEN, PRIVACY LAW AND SOCIETY 846 (2007).
[50] Los Angeles Air Force Base, *Global Positioning System Fact Sheet*, *available at* http://web.archive.org/web/20090119020458/http://www.losange les.af.mil/library/factsheets/factsheet.asp?id=5325.
[51] National Geospatial-IntelligenceAgency, *Current GPS Satellite Data*, *available at* http://earth-info.nga.mil/GandG/sathtml/satinfo.html.
[52] *Global Positioning System Fact Sheet*, supra note 14.
[53] *Id.*
[54] *Id.*

enough to be installed almost anywhere and still maintain full functionality.[55] GPS receivers can remain connected to satellites in spite of physical barriers, functioning in "tree canopies or in canyons, on country roads or beneath sky scrapers."[56] In the world of the "Internet of Things," GPS therefore adds the ability of devices to be physically tracked almost anywhere.

In addition to GPS devices specifically purchased for navigational purposes, GPS technology appears in a variety of other commonplace devices that consumers use every day. For instance, some cars are beginning to come equipped with "Event Data Recorders," or EDRs. EDRs are electronic "black boxes" that collect and store information about the operation of a motor vehicle.[57] The data recorded might include the date, time, velocity, direction, number of occupants, airbag data, seat belt use, and location data. While some EDRs rely on cellular technology in order to collect data, others, such as the MacBox system tested by the Drive Atlanta project at the Georgia Institute of Technology, rely on GPS to collect and monitor users' driving habits and location.[58]

II. Privacy and Security Risks of the Internet of Things

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

One of the primary risks that internet users will face as the Internet of Things expands is the fact 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.[59] A "Smart Grid" is an electrical or power grid that is equipped with

[55] GPS for Today, *Small GPS Tracking Chips*, Dec. 21, 2009, *available at* http://www.gpsfortoday.com/small-gps-tracking-chips/.
[56] *Id.*
[58] Electronic Privacy Information Center, Comments to the National Highway Traffic Safety Administration, Docket No. NHTSA-2002-13546, Feb. 28, 2003, at 2.
[58] *Id.*
[59] Electronic Privacy Information Center, Comments to the National Institute of Standards and Technology, "NIST Framework and Roadmap for Smart Grid Interoperability Standards Release 1.0," Nov. 9, 2009, at 4.

telecommunications and internet technologies used specifically to track user behavior in order to increase efficiency, sustainability, and economy.[60] Thus, a region's smart grid could track in realtime 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.[61] However, the capability of a Smart Grid to track consumer behavior so closely poses a serious privacy risk. Information about a power consumer's schedule can reveal intimate, personal details about their lives, such as their medical needs, interactions with others, and personal habits.[62] That concern is further exacerbated by the fact that Smart Grid meter data may be able to track the use 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.[63]

Other sensitive behavior patterns may be illustrated through the data collected by EDRs. The National Highway Traffic Safety Administration has proposed that, beginning September 1, 2014, all new cars will be required to have EDRs. [64] The data that the devices record can be made available to insurance companies, the police, and other third parties.[65] Currently, there are minimal privacy protections in the draft regulation. Since cars, like cell phones, have become increasingly unique to one user, the information collected by EDRs in the coming years will be able to tell an increasingly personal story about automobile owners. EDRs will record not just the

[60] 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).
[61] *Id*.
[62] EPIC Comments, supra note 60, at 4-5.
[63] *Id*. at 5.
[64] Press Release, National Highway Traffic Safety Administration, U.S. DOT Proposes Broader Use of Event Data Recorders to Help Improve Vehicle Safety (Dec. 7, 2012), available at http://www.nhtsa.gov/About+NHTSA/Press+Releases/U.S.+DOT+Proposes+Broader+Use+of+Event+Data+Recorders+to+Help+Improve+Vehicle+Safety.
[65] Electronic Privacy Information Center, Comments to the National Highway Traffic Safety Administration, Docket No. NHTSA-2002-13546, Feb. 28, 2003, at 2.

number of miles a consumer drives, or the maximum speed the driver attains, but also more granular details, like the speed the consumer attains on certain roads at certain times.[66] As EDR technology merges with built-in GPS technology, personal cars may be able to record every aspect of the driver's activity. This kind of data poses enormous privacy risks to drivers; an EDR could reveal where a driver goes, at what time of day, the route the driver takes, and based on speeding habits, how urgently the driver wished to arrive there.[67] As EDRs become a regular part of the Internet of Things, drivers will have to become accustomed to the fact that data collected by their cars can reveal the frequency and location of hospital trips, therapy sessions, personal visits, or even daily lunch habits.

B. Data Collected from the Internet of Things Could be Used for Secondary Purposes Which Lack 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.[68] Because the Internet of Things will generate data from all aspects of consumers' lives, these types of secondary uses could lead to the commercialization of intimate segments of consumers' lives.

Commercial secondary uses have already occurred in a number of contexts. For example, General Motors announced in 2011 that data generated by OnStar, a vehicle-based communications, security, and navigation system, could be sold to marketers, local governments,

[66] *Id*. at 3.
[67] *See id.* at 3-4.
[68] *Comments of EPIC to NIST, NIST Framework and Roadmap for Smart Grid Interoperability Standards Release 1.0 (Draft)* EPIC, 8 (2009) (describing use of smart grid for advertising).

or location-based service companies.[69] Companies like Euclid allow retailers to use Wi-Fi access points to track the foot traffic of consumers through the location of their Wi-Fi enabled smartphones.[70] Recently, Verizon announced that it would sell consumers' smartphone data, including demographics, app usage, and location information.[71] Verizon also recently had a patent rejected that would have used a TV set-top box to target ads based on the speech and actions of the TV viewers.[72] Finally, for several years the Internet browsing data of consumers has been used by a number of third parties to target advertisements.[73]

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 by, and may be changed at will by, the companies. These "take it or leave it" arrangements dominate the market for many important services, and, as the Commission itself has recognized, they leave consumers relatively disempowered and without meaningful choice.[74]

---

[69] John R. Quain, *Changes to OnStar's Privacy Terms Rile Some Users*, N.Y. TIMES, Sept. 22, 2011, http://wheels.blogs.nytimes.com/2011/09/22/changes-to-onstars-privacy-terms-rile-some-users

[70] Quentin Hardy, *Technology Turns to Tracking People Offline*, N.Y. TIMES, (March 7, 2013), http://bits.blogs.nytimes.com/2013/03/07/technology-turns-to-tracking-people-offline/

[71] Jessica Leber, *How Wireless Carriers are Monetizing your Movements*, TECHNOLOGY REVIEW (Apr. 12, 2013), http://www.technologyreview.com/news/513016/how-wireless-carriers-are-monetizing-your-movements/

[72] Jeremy Hsu, *Verizon Idea to Track TV Viewers Gets Patent Rejection*, TechNews Daily (Dec. 12, 2012), http://www.technewsdaily.com/15896-verizon-tv-patent-rejection.html

[73] Chris Jay Hoofnagle et. al, *Behavioral Advertising: The Offer that You Cannot Refuse*, 6 HARVARD LAW & POLICY REVIEW 273 (2012)

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

The Internet of Things could increase the relative power of companies by providing them with more information about consumers. Information is power, and smart devices will provide much more information 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 utilize it more effectively.[75]

This concentration of power has important implications for the security of consumers' personal data. For example, technologist and security expert Bruce Schneier has described the "feudal model" of security that results 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."[76] This type of feudalism is being driven by many factors, but one of the main developments cited by Schneier 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.[77] This influence or direction may take many

---

[75] 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)

[76] 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/

[77] 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")

forms, and may be accomplished through a variety of consumer devices. For example, insurance companies might use Event Data Recorders to adjust insurance rates according to driving behavior.[78] "The aim is to both punish driving patterns that are considered to be "risky" and to modify driving behavior through the constant surveillance enabled by EDR technology."[79] Similarly, the increased amount of usage data will enable companies to develop and enforce hidden charges and fees for certain uses. For example, GPS and other networked technologies have enabled rental car companies to charge numerous "gotcha fees" for driving outside of specified regions or using certain services.[80]

Finally, companies might exercise their power over consumers through profiling. Rather than influencing or incentivizing behavioral change, profiling tends to be status-based, assigning consumers to certain categories from which it is difficult to escape.[81] For example, companies might rank consumers by desirability, separating them into high-value prospects and "waste" and channeling better offers, services, and benefits to those at the top. The New York Times describes how one data broker was able to help a national prepaid debit card issuer assign scores to potential customers and target only those who scored high enough to be considered "highly profitable customers."[82] These risks echo those that led to the Commission's ongoing investigation into the business practices of several data brokers.[83]

---

[78] Electronic Privacy Information Center, Comments to the National Highway Traffic Safety Administration, Docket No. NHTSA-2002-13546, Feb. 28, 2003, at 3.
[79] *Id.*
[80] *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
[81] Natasha Singer, *Secret E-Scores Chart Consumers' Buying Power*, N.Y. TIMES (Aug. 18, 2012), https://www.nytimes.com/2012/08/19/business/electronic-scores-rank-consumers-by-potential-value.html?pagewanted=all ("But the spread of consumer rankings raises deep questions of fairness, says Frank Pasquale, a professor at Seton Hall University School of Law, who is writing a book about scoring technologies. The scores may help companies, he says. But over time, they may send some consumers into a downward spiral, locking them into a world of digital disadvantage.")
[82] *Id.*
[83] Press Release, Fed Trade Comm'n, FTC to Study Data Broker Industry's Collection and Use of Consumer Data (Dec. 18, 2012), http://www.ftc.gov/opa/2012/12/databrokers.shtm

D. The Internet of Things has the Potential to Threaten the Users' Security, Both On and Offline

A final risk to consumers in the Internet of Things will be security, both of the users' data, and of their physical person. As an initial matter, many of the same data security risks that currently threaten our data will only expand in the Internet of Things. The damage caused by malware, phishing, spam and viruses will have an increasingly large array of networks in which to spread.[84] Additionally, not all wireless connections in the Internet of Things will be encrypted.[85] For instance, one of the ways EDR data is accessed is through the Onboard Diagnostic connector (OBD-II). The OBD-II was federally-mandated to allow access to engine and emissions diagnostics data, but has become a central access point to a number of on-vehicle computers. Most modern vehicles have an OBD-II port located under the dash.[86] However, the OBD-II is not universally physically secure, which may allow access and manipulation of EDR data. Further, EDRs, as well as lightweight vehicle's wireless and non-wireless computer systems, are routinely not encrypted. [87] Physical access to the OBD-II is not required to compromise the computer systems of a vehicle and consequently the EDR data. The same compromising of computer systems in vehicles can occur via the physical port or hacking through a wireless signal.[88]

In addition to the risks to data security, the physical security of persons and their property may also be at risk in the Internet of Things. This is particularly true given that the constant flow

---

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

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

[86] Hampton C. Gabler, *et. al., Use of Event Data Recorder (EDR) Technology for Highway Crash Data Analysis* 97 (Dec. 2004), *available at* www.harristechnical.com/downloads/nchrp_w75.pdf. *See also* https://epic.org/privacy/edrs/EPIC-Coal-NHTSA-EDR-Cmts.pdf.

[87] Karl Koscher, *et. al., Experimental Security Analysis of a Modern Automobile* 1 (2010), *available at* www.autosec.org/pubs/cars-oakland2010.pdf.

[88] *Id*. at 4.

of data will so easily delineate sensitive behavior patterns, and will flow over networks that are not always secure, leaving them vulnerable to malicious hackers.[89] For instance, a hacker could monitor a consumer's Smart Grid power use to determine when the consumer is at work, allowing the hacker to more easily burgle the house. Similarly, a hacker who gains access to the data transmitted via OBD-II could determine when a driver is in a particularly remote or isolated area, if the hacker wished to assault or rob the driver.[90] The lines of communication that link the Internet of Things will need to be strengthened and more carefully scrutinized. As the Carnegie Mellon Engineering Department has noted, "Some of this communication will take place over wires or fiber optics. Some of it will involve wireless connections. All of these communication links introduce vulnerabilities, especially if they can be accessed over the Internet."[91]

III. Recommendations for Addressing the Privacy and Security Risks of the Internet of Things

A. The Commission Should Require Companies That Collect Data From Smart Devices to Implement the Principles of Privacy By Design

The Commission has frequently advocated in favor of companies adopting "privacy by design" as a method for encouraging consumer privacy in the United States.[92] "Privacy by design," or the process of embedding privacy protections throughout every stage of the development of a technology, contemplates that the technology itself will limit consumer data collection.[93] Rather than building an EDR that is capable of storing potentially limitless travel records, for instance, a regime of privacy by design would automatically delete old data after a certain amount of time, or prevent individual data from being automatically synched with a

[89] M. Granger Morgan, et. al, The Many Meanings of "Smart Grid," 5 (2009), *available at* http://www.epp.cmu.edu/Publications/Policy_Brief_Smart_Grid_July_09.pdf
[90] Federal Motor Vehicle Safety Standards; Event Data Recorders, Docket No. NHTSA-2012-0177 (Comments of Privacy Coalition), 10-11 *available at* https://epic.org/privacy/edrs/EPIC-Coal-NHTSA-EDR-Cmts.pdf.
[91] Morgan at 5.
[92] FED. TRADE COMM'N, PROTECTING CONSUMER PRIVACY IN AN ERA OF RAPID CHANGE 22-35 (2012), http://www.ftc.gov/os/2012/03/120326privacyreport.pdf.
[93] *Id*.

central database.[94] There are several well-established methods of achieving privacy by design, and in the Internet of Things, all of these methods will be necessary.

B. The Commission Should Protect Consumers Rights to Limit Data Collection and Use

The Commission should require that companies secure consumer consent before using data for secondary purposes. For example, in the case of the smart grid, consent would be required for collection and use outside of that necessary to the provision of the service. Consent is a foundational privacy practice. Moreover, this practice mirrors the Commission's previous recommendations. For example, the 2012 privacy report recommends that "for practices inconsistent with the context of their interaction with consumers, companies should give consumers choices."[95]

Importantly, for consent to be effective, companies must not be allowed to condition use of a service on unnecessary data collection. This is the approach recommended by the Article 29 Working Party,[96] and by at least one state in the context of Event Data Recorders.[97] The Commission also recognizes that binary, "take it or leave it" choices undermine consumer consent. In its privacy report, the Commission notes that such an approach "is problematic from a privacy perspective in markets for important services where consumers have few options."[98]

C. The Commission Should Emphasize Transparency, Access, and Accuracy for Data Generated by Smart Devices

---

[94] 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).

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

[96] *See* ARTICLE 29 DATA PROTECTION WORKING PARTY, OPINION 15/2011 ON THE DEFINITION OF CONSENT 2011, http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2011/wp187_en.pdf

[97] *See* Va. Code Ann. § 38.2-2213.1 (West) (prohibiting insurance companies from reducing coverage, increasing premiums, applying surcharges, or denying discounts solely because a vehicle operator or owner refuses to grant her insurance company access to EDR data.)

[98] FED. TRADE COMM'N, PROTECTING CONSUMER PRIVACY IN AN ERA OF RAPID CHANGE 67 (2012), http://www.ftc.gov/os/2012/03/120326privacyreport.pdf

The Commission should require companies that collect data from smart devices to provide transparency regarding their data collection practices, and access to this data for consumers. Many of the consumer benefits[99] 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 computer, such as a 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.[100]

These principles have been widely embraced by among the privacy community and by the Commission itself. The EU Data Protection Directive, for example, grants data subjects a "right of access" to the logic involved in any automatic processing of personal data.[101] Similarly, the Article 29 Working Party Opinion on Smart Metering recommends that data controllers respect the rights of data subjects to access and correct the data generated by smart meters.[102] Finally, both the Department of Commerce and the Commission have also cited transparency,

[99] *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/.
[100] *Id*.
[101] Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, 1995 O.J. (L 281) art. 12(a) *available at* http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:1995:281:0031:0050:EN:PDF.
[102] *See* ARTICLE 29 DATA PROTECTION WORKING PARTY, OPINION 12/2011 ON SMART METERING 2011, http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2011/wp183_en.pdf.

access, and accuracy as essential elements of privacy protection.[103] Thus, these principles should be incorporated into any best practices guide for the Internet of Things.

D. The Commission Should Require Data Minimization Practices from Companies that Collect Data Generated By Smart Devices

The Commission should require companies to adopt the principle of data minimization, so that companies that collect user data only store and use so much data as is necessary to ensure the functionality of their products or services.[104] 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 - that is, storing individual data only for as long as it takes to develop an aggregate computation - could allow for a very accurate aggregation, while ensuring a degree of anonymity for the consumers. Data retention periods should be restricted as well.

IV. Conclusion

The Internet of Things presents important implications for consumer privacy and security. By recommending best practices early, the Commission can ensure these technologies are implemented in a way that benefits consumers and respects important values. EPIC welcomes the opportunity to work with the Commission in the future on this issue.

---

[103] *See* WHITE HOUSE, CONSUMER DATA PRIVACY IN A NETWORKED WORLD: A FRAMEWORK FOR PROTECTING PRIVACY AND PROMOTING INNOVATION IN THE GLOBAL ECONOMY 2012, http://www.whitehouse.gov/sites/default/files/privacy-final.pdf; FED. TRADE COMM'N, PROTECTING CONSUMER PRIVACY IN AN ERA OF RAPID CHANGE (2012), http://www.ftc.gov/os/2012/03/120326privacyreport.pdf.

[104] *Id*. at 23-24.

Respectfully Submitted,

Marc Rotenberg, EPIC President and Executive Director
David Jacobs, EPIC Consumer Protection Counsel
Julia Horwitz, EPIC Open Government Fellow

Electronic Privacy Information Center
1718 Connecticut Ave. NW Suite 200
Washington, DC 20009
202-483-1140 (tel)
202-483-1248 (fax)