BEFORE THE
DEPARTMENT OF COMMERCE
NATIONAL TELECOMMUNICATIONS & INFORMATION ADMINISTRATION

In the Matter of
The Benefits, Challenges, and Potential Roles for the Government in Fostering the Advancement of the Internet of Things

Docket No. 160331306-6306-01

Comments of the Staff of the Federal Trade Commission's Bureau of Consumer Protection and Office of Policy Planning

June 2, 2016

I. INTRODUCTION

The staff of the Federal Trade Commission's ("FTC") Bureau of Consumer Protection ("BCP") and Office of Policy Planning ("OPP") (hereafter "staff')[1] appreciate this opportunity to comment on the Department of Commerce, National Telecommunications and Information Administration ("NTIA") Request for Comment ("RFC") on the Internet of Things ("Internet of Things" or "IoT").[2] In part, the RFC seeks to: (1) define the Internet of Things;[3] (2) understand the security and privacy issues related to IoT;[4] (3) understand the technical issues surrounding standardization and interoperability;[5] and (4) understand the impact that big data in an interconnected world can have on disadvantaged communities.[6] This comment highlights lessons learned from the FTC's law enforcement, consumer and business education, and policy activities relating to these issues. It then addresses the benefits and risks of IoT, highlights some best practice recommendations for industry, discusses the role of government in fostering innovation in IoT products and services, and sets forth some considerations for NTIA in setting standards and promoting interoperability.

II. BACKGROUND ON THE FTC

The FTC is an independent administrative agency responsible for protecting consumers and promoting competition. As part of its consumer protection mandate, the FTC enforces a wide range of laws to protect the privacy and security of consumer data. The primary law enforced by the FTC, the FTC Act, prohibits "unfair" and "deceptive" acts or practices in or affecting commerce, including unfair and deceptive privacy and security practices.[7] The FTC also enforces sector-specific statutes that protect certain health, credit, financial, and children's information, and has issued regulations implementing each of these statutes.[8]

To date, the FTC has brought over 500 cases protecting the privacy and security of consumer information, including cases against well-known companies such as Twitter, Facebook, Google, Snapchat, HTC, and router manufacturer ASUS.[9] The FTC's enforcement actions send an important message to companies about the need to protect consumers' privacy and data security.

---

[1] These comments represent the views of the staff of the Bureau of Consumer Protection and Office of Policy Planning. The Commission has, however, voted to authorize the staff to submit these comments.
[2] 81 Fed. Reg. 19956 (April 6, 2016).
[3] *Id.* at 19958 (Questions 2 and 4).
[4] *Id.* at 19959 (Questions 15-17).
[5] *Id.* (Question 6).
[6] *Id.* (Question 19).
[7] 15 U.S.C. § 45(a).
[8] *See, e.g.*, Health Breach Notification Rule, 16 C.F.R. Part 318 *et seq.* (health information breach notification); Fair Credit Reporting Act, 15 U.S.C. § 1681 *et seq.* and 16 C.F.R. Part 600 (consumer reporting information security and privacy); Gramm-Leach-Bliley Act Safeguards Rule, 16 C.F.R. Part 314 *et seq.* (financial information security); Children's Online Privacy Protection Act of 1998, 15 U.S.C. § 6501 *et seq.* and 16 C.F.R. Part 412 (children's online information security and privacy).
[9] Letter from Edith Ramirez, Chairwoman, Fed. Trade Comm'n, to Věra Jourová, Commissioner for Justice, Consumers and Gender Equality, European Commission, at 3 (Feb. 23, 2016), *available at* https://www.ftc.gov/system/files/documents/public_statements/927423/160229ftc_privacyshieldletter.pdf.

The FTC also has pursued numerous policy initiatives designed to enhance consumer privacy. For example, the FTC has hosted workshops and issued reports to improve privacy disclosures in the mobile ecosystem, increase transparency in the data broker industry, examine the implications of big data on low-income and underserved consumers, and highlight the privacy and security implications of facial recognition and the Internet of Things.[10]

Finally, the FTC engages in consumer and business education to increase the impact of its enforcement and policy development initiatives. The FTC uses a variety of tools – brochures, online resources, workshops, and social media – to distribute educational materials on a wide range of topics, including mobile apps, children's privacy, and data security. On the business education front, most recently, the Commission launched its "Start with Security" initiative and "Careful Connections" IoT guidance, both of which include some lessons for businesses considering security issues in the IoT space.[11] On the consumer education front, the FTC recently announced the rollout of its enhanced IdentityTheft.gov website,[12] a free, one-stop resource people can use to report and recover from identity theft. Now, identity theft victims can use the site to create a personal recovery plan based on the type of identity theft they face, and get pre-filled letters and forms to send to credit bureaus, businesses, debt collectors, the IRS and others.

As part of its competition mandate, the FTC has a more than 30-year history of examining the role of standardization and interoperability in technology markets, with a particular emphasis on competitive and innovation effects.[13] For example, the FTC has studied competition issues relating to interoperability in networked industries[14] and considered how the evolution of interoperable technology can impact consumers of information technology.[15] The FTC also has studied competition in markets shaped by interoperability, such as business-to-

---

[10] *See, e.g.*, FED. TRADE COMM'N, INTERNET OF THINGS: PRIVACY AND SECURITY IN A CONNECTED WORLD (Jan. 2015) (report), *available at* https://www.ftc.gov/system/files/documents/reports/federal-trade-commission-staff-report-november-2013-workshop-entitled-internet-things-privacy/150127iotrpt.pdf [hereinafter IoT Report]; *see also* FED. TRADE COMM'N, INTERNET OF THINGS: PRIVACY AND SECURITY IN A CONNECTED WORLD (Nov. 19, 2013) (workshop), *available at* https://www.ftc.gov/news-events/events-calendar/2013/11/internet-things-privacy-security-connected-world [hereinafter IoT Workshop].

[11] Fed. Trade Comm'n, Start with Security: A Guide for Business (June 2015) [hereinafter Start with Security], *available at* https://www.ftc.gov/tips-advice/business-center/guidance/start-security-guide-business; Fed. Trade Comm'n, *Careful Connections: Building Security in the Internet of Things* (Jan. 2015) [hereinafter Careful Connections], *available at* https://www.ftc.gov/tips-advice/business-center/guidance/careful-connections-building-security-internet-things.

[12] *See* Press Release, FTC, FTC Announces Significant Enhancements to IdentityTheft.gov (Jan. 28, 2016), *available at* https://www.ftc.gov/news-events/press-releases/2016/01/ftc-announces-significant-enhancements-identitytheftgov; *see also* https://robodeidentidad.gov/ in Spanish).

[13] *See, e.g.*, FED. TRADE COMM'N BUREAU OF CONSUMER PROT., FINAL STAFF REPORT: STANDARDS AND CERTIFICATION (1983); Brief for United States & Fed. Trade Comm'n as Amici Curiae Supporting Respondent, *Allied Tube & Conduit Corp. v. Indian Head, Inc*. 486 U.S. 492 (1987) (No. 87–157); *In re American Society of Sanitary Engineering*, 106 F.T.C. 324 (1985).

[14] *See* FED. TRADE COMM'N STAFF, ANTICIPATING THE 21ST CENTURY: COMPETITION POLICY IN THE NEW HIGH-TECH, GLOBAL MARKETPLACE (1996).

[15] FED. TRADE COMM'N STAFF, PROTECTING CONSUMERS IN THE NEXT TECH-ADE (2008).

business ("B2B") electronic marketplaces[16] and the deregulated market for electricity.[17] And, last year, the FTC provided comments on the Office of the National Coordinator for Health Information Technology draft Shared Nationwide Interoperability Roadmap, which laid out a plan to promote the adoption of interoperable health information technology systems.[18] Most recently, the FTC has studied the impact of patented technologies on the interoperability standards prevalent in the telecommunications industry.[19] Finally, the FTC has brought enforcement actions against parties based upon misrepresentations made during the standard setting process.[20]

III. THE BENEFITS AND RISKS OF THE INTERNET OF THINGS

The Internet of Things refers to the ability of everyday objects to connect to the Internet to send and receive data.[21] The IoT includes consumer-facing devices—such as smartphones, cameras, appliances, and wearable health devices—as well as non-consumer-facing devices, such as those designed for businesses to enable automated communications between machines. For example, the term IoT can include machine-to-machine communications that enable businesses to track inventory; sensor networks to monitor electricity use in hotels; and Internet-connected jet engines and drills on oil rigs.[22] While such business or industrial IoT communications may affect consumers, this comment is limited to devices that are sold to or used by consumers.

In November 2013, the FTC held a workshop, titled *The Internet of Things: Privacy and Security in a Connected World*. At the workshop, panelists from government, industry, and consumer groups discussed "The Smart Home," "Connected Health and Fitness," "Connected Cars," and the issue of "Privacy and Security."[23] In January 2015, FTC staff issued a comprehensive report offering substantive recommendations, based on the workshop transcript and comments received as part of the workshop record. The FTC's report on the Internet of Things addressed many of the issues raised by NTIA's RFC, including the benefits and risks associated with IoT devices, and the role of the FTC in fostering innovation while protecting

[16] FED. TRADE COMM'N STAFF, ENTERING THE 21ST CENTURY: COMPETITION POLICY IN THE WORLD OF B2B ELECTRONIC MARKETPLACES (2000).
[17] *See, e.g.*, FED. TRADE COMM'N STAFF, COMPETITION AND CONSUMER PROTECTION PERSPECTIVES ON ELECTRIC POWER REGULATORY REFORM (2000).
[18] *See* Comment of the Staff of the Office of Policy Planning, Bureau of Competition, Bureau of Economics and Bureau of Consumer Protection of the Fed. Trade Comm'n before the Office of the National Coordinator for Health Information Technology (April 3, 2015). While that comment raised several of the same general observations regarding interoperability and standardization as raised below, the specific costs and benefits of adopting interoperability may vary between industries and should be evaluated on a case-by-case basis.
[19] FED. TRADE COMM'N, THE EVOLVING IP MARKETPLACES: ALIGNING PATENT NOTICE AND REMEDIES WITH COMPETITION (2011); FED. TRADE COMM'N AND U.S. DEP. JUSTICE, ANTITRUST ENFORCEMENT AND INTELLECTUAL PROPERTY RIGHTS: PROMOTING INNOVATION AND COMPETITION (2007) [hereinafter 2007 IP Report].
[20] *See, e.g.*, Complaint, *In re Dell*, 121 F.T.C. 616, 616-18 (1996) (No. C-3658) (resolved by consent order, 121 F.T.C. at 618-26); Complaint, *In re Rambus, Inc.*, No. 9302 (F.T.C. June 18, 2002); Complaint, *In re Union Oil Co. of Cal.*, No. 9305 (F.T.C. Mar. 4, 2003) (resolved by consent order, No. 9305 (F.T.C. July 27, 2005)).
[21] IoT Report at 6.
[22] *Id.* at 5-6.
[23] IoT Workshop, *supra* note 10.

consumers. This comment summarizes many of the findings and recommendations from the IoT Workshop and IoT Report.

A. Benefits

The Internet of Things promises revolutionary benefits to the way consumers live and interact with the world. For example, in the area of connected health, consumer-facing products such as insulin pumps and blood-pressure cuffs can enable people to record, track, and monitor their own vital signs, without having to go to a doctor's office. This can be especially beneficial for aging patients, allowing them to manage their health care at home.[24]

In the home, smart meters can enable consumers to analyze their energy use and identify issues with home appliances, which can lead to greater energy efficiency and reduced costs. Home automation systems can provide consumers with a single platform that can connect all of the devices within the home. Sensors known as "water bugs" can notify consumers if their basements have flooded, and thermostats can automatically adjust temperature settings depending on the time of day and presence of people in the house.[25]

On the road, connected cars increasingly offer many safety and convenience benefits to consumers. For example, sensors on a car can notify drivers of dangerous road conditions or obstacles. Connected cars also can offer real-time vehicle diagnostics to drivers and service facilities; Internet radio; navigation, weather, and traffic information; automatic alerts to first responders when airbags are deployed; and smartphone control of the starter and other aspects of the car. In the near future, some cars might even drive themselves.[26]

Beyond providing benefits to individuals, IoT devices may collect and aggregate data that can provide benefits to society. For example, big data analysis of information collected from connected health devices can facilitate health research and lead to breakthroughs in treatment. Similarly, analysis of data collected from a connected public infrastructure to detect, for example, the lighting patterns on public streets, can help improve energy efficiency.[27] These types of analyses can also help target public service messages and resources to relevant populations, including low-income and disadvantaged communities.

As these examples illustrate, IoT devices can provide vast benefits and opportunities to consumers. New, unexpected, and beneficial uses for the data derived from these devices emerge every day.

---

[24] IoT Report at 7.
[25] *Id.* at 8-9.
[26] *Id.* at 9.
[27] WHITE HOUSE, BIG DATA: SEIZING OPPORTUNITIES, PRESERVING VALUES 39-40 (May 2014) (report), *available at* http://www.whitehouse.gov/sites/default/files/docs/big_data_privacy_report_5.1.14_final_print.pdf.

B. Risks

Despite these benefits, the IoT raises security and privacy risks, described below.

1. Security Risks

IoT devices may present a variety of security risks. FTC staff's IoT Report describes in greater detail the range of security risks and practices.[28] Although similar risks exist with traditional computers and computer networks, they may be heightened in the IoT, in part because many IoT chips are inexpensive and disposable, and many IoT devices are quickly replaceable with newer versions. As a result, businesses may not have an incentive to support software updates for the full useful life of these devices, potentially leaving consumers with vulnerable devices.[29] Moreover, it may be difficult or impossible to apply updates to certain devices.[30]

Security risks in IoT can be exploited to harm consumers by: (1) enabling unauthorized access and misuse of personal information; (2) facilitating attacks on other systems; and (3) creating safety risks. First, on IoT devices, as with desktop or laptop computers, a lack of security can enable intruders to access and misuse personal information collected or stored on a device. As IoT devices offer new opportunities for consumers to monitor their daily activities, access content, and interact with the world, these devices also create new opportunities for unauthorized persons to exploit vulnerabilities that can facilitate identity theft or fraud.[31]

Second, by definition, IoT devices must be capable of being connected to the Internet. As such, security vulnerabilities in a particular IoT device can act as entry points for attacks into consumers' or business' networks, likely increasing exposure to security risks across entire systems.[32]

Third, security vulnerabilities in IoT devices can potentially lead to not only data security risks but also threats to a person's physical safety. For example, vulnerabilities in an IoT insulin pump or pacemaker can result in significant injury or even death to a consumer; an attack on a

---

[28] *See generally* IoT Report at 10-14.

[29] *See, e.g.*, Article 29 Data Protection Working Party, Opinion 8/2014 on Recent Developments on the Internet of Things 9 (Sept. 16, 2014) ("Article 29 Working Group Opinion"), *available at* http://ec.europa.eu/justice/dataprotection/article-29/documentation/opinion-recommendation/files/2014/wp223_en.pdf ("For example, most of the sensors currently present on the market are not capable of establishing an encrypted link for communications since the computing requirements will have an impact on a device limited by low-powered batteries."); Meghan Neal, *The Heartbleed Bug Will Lurk in the Internet of Things for Decades* (Apr. 11, 2014), http://motherboard.vice.com/read/the-heartbleed-bug-will-lurk-in-the-internet-of-things-for-decades.

[30] IoT Report at 13. This could be because some devices may not have the computing power to establish an encrypted communications link to receive updates. In addition, it may be difficult to notify consumers of security updates for devices that do not have a screen.

[31] *Id.* at 10-11.

[32] *Id.* at 11-12. Further, as IoT devices proliferate, vulnerabilities can enable attackers to assemble large numbers of devices to launch denial of service attacks.

vulnerable connected car can lead to engine failure or a loss of control; and an insecure IoT alarm system can open up a home to danger.[33]

2. Privacy Risks

Beyond security risks, IoT devices also raise concerns about consumer privacy. Some privacy risks involve the direct collection of sensitive personal information, such as precise geolocation, financial account numbers, or health information.[34] Others arise from the collection of personal information, habits, locations, and physical conditions over time, which may allow an entity that has not directly collected sensitive information to infer it.[35]

In one FTC analysis, staff found the presence of numerous third parties in apps connected to IoT health and fitness wearable devices.[36] A number of those third parties collected data such as persistent device identifiers, workout routines, eating habits, length of walking stride, medical search histories, zip code, gender, and geolocation. As this analysis demonstrates, IoT devices are capable of collecting, transmitting, and sharing highly sensitive information about consumers' bodies and habits. These privacy implications may increase if consumers' health routines, dietary habits, and medical searches are combined with offline sources and across devices.[37]

The IoT impacts other types of sensitive information beyond health and fitness, including information about children. The market for children's IoT devices has expanded into areas of safety, education, sports, entertainment and beyond.[38] This explosion of children's IoT devices also raises concerns about children's privacy and security, including how to protect children's photos and audio recordings and how to restrict access to children's accounts.[39] In the United

---

[33] *Id.* at 12-13. *See e.g.* Andy Greenberg, "Hackers Cut a Corvette's Brakes Via A Common Car Gadget," WIRED (August 11, 2015), available at https://www.wired.com/2015/08/hackers-cut-corvettes-brakes-via-common-car-gadget; Aliya Sternstein, *FBI and DHS Warn of Security Risks From the Internet of Things* (Sept. 14, 2015), *available at* http://www.nextgov.com/cybersecurity/2015/09/these-are-10-things-internet-things-fbi-and-dhs-are-warning-about/120884/.

[34] IoT Report at 14.

[35] *Id.*

[36] FED. TRADE COMM'N, CONSUMER GENERATED AND CONTROLLED HEALTH DATA (May 2014) (workshop), *available at* https://www.ftc.gov/system/files/documents/public_events/195411/consumer-health-data-webcast-slides.pdf. *See also,* FED. TRADE COMM'N, DATA BROKERS: A CALL FOR TRANSPARENCY AND ACCOUNTABILITY (May 2014) (report), *available at* https://www.ftc.gov/reports/data-brokers-call-transparency-accountability-report-federal-trade-commission-may-2014 ("For example, businesses can purchase their customers' email addresses from data brokers so that they can send email solicitations to them. They can also purchase information about their customers' interests in order to market specific products to them, including using consumers' offline activities to determine what advertisements to serve them on the Internet.").

[37] *Id. See also*, PRIVACY RIGHTS CLEARINGHOUSE, MOBILE HEALTH AND FITNESS APPLICATIONS AND INFORMATION PRIVACY (July 2013), *available at* https://www.privacyrights.org/mobile-medical-apps-privacy-consumer-report.pdf.

[38] Lindsay Boeckl, *The Future of Wearables for Kids* (Dec. 14, 2015), *available at* https://medium.com/@ConnectedLab/when-i-was-your-age-pluto-was-still-a-planet-8bc6dfc356cf#.3ynkcx79l.

[39] *See e.g.* Becky Slack, *Is the Internet of Things Putting Your Child's Privacy at Risk* (Feb. 29, 2016), *available at* http://www.theguardian.com/sustainable-business/2016/feb/29/is-the-internet-of-things-putting-your-childs-privacy-at-risk.

States, the FTC is responsible for enforcing the Children's Online Privacy Protection Act[40] and continues to protect the personal information of children through robust enforcement[41] and industry guidance.[42] To this end, the FTC has brought approximately 25 cases alleging COPPA violations, issued and updated a comprehensive set of FAQs on COPPA, and provided additional education through blog posts and speeches.

The massive volume of granular data collected by IoT devices enables those with access to the data to perform analyses that would not be possible with less rich data sets. For example, car insurance companies can now use data from connected cars to base insurance rates on consumers' actual driving habits (e.g., number of "hard brakes," miles driven, and amount of time driving between midnight and 4 a.m.); others might use IoT data to make in-house credit, insurance, or other eligibility-type decisions.[43] Using data for these purposes could bring benefits, such as enabling safer drivers to reduce their rates for car insurance or expanding consumers' access to credit. However, such uses could be problematic if they occurred without consumers' knowledge or consent, or without regard to the accuracy of the data.

In addition to the volume of data that can be collected by a single IoT device, the ability to link and associate multiple IoT devices to the same user can also pose material privacy risks. With advancements in IoT and cross-device tracking, the potential exists for companies to associate information about users across devices. For example, a consumer who wears an IoT fitness band to monitor her sleeping patterns might also drive a connected car to alert her family in real-time about where she is driving, use a set-top box to stream action movies over the Internet, and use IoT "water bugs" to alert her when the faucet is left running for too long. The potential for a cross-device tracking company to associate and aggregate information about consumers' sleeping patterns, driving habits, movie preferences, and household activities implicates privacy risks not previously contemplated in the era of desktop computers.

In November 2015, FTC staff held a workshop on Cross-Device Tracking discussing these issues.[44] At the workshop, FTC staff presented findings showing that cross-device tracking companies were present on a considerable majority of the websites they studied and that 90

---

[40] 15 U.S.C. 6501 *et seq.*

[41] *See, e.g.*, Fed. Trade Commission, *Kids Privacy (COPPA) Page*, *available at* https://www.ftc.gov/news-events/media-resources/protecting-consumer-privacy/kids-privacy-coppa.

[42] FED. TRADE COMM'N, KIDS' APPS DISCLOSURES REVISITED (Sept. 3, 2015) (blog), *available at* https://www.ftc.gov/news-events/blogs/business-blog/2015/09/kids-apps-disclosures-revisited; FED. TRADE COMM'N, MOBILE APPS FOR KIDS: DISCLOSURES STILL NOT MAKING THE GRADE (Dec. 2012) (staff report), *available at* https://www.ftc.gov/reports/mobile-apps-kids-disclosures-still-not-making-grade; and FED. TRADE COMM'N, MOBILE APPS FOR KIDS: CURRENT PRIVACY DISCLOSURES ARE DISAPPOINTING (Feb. 2012) (staff report), *available at* https://www.ftc.gov/reports/mobile-apps-kids-current-privacy-disclosures-are-disappointing.

[43] IoT Report at 16-17. While the Fair Credit Reporting Act ("FCRA") imposes certain limits on the use of consumer data in making determinations about credit, insurance, or employment, or for similar purposes, the statute only extends to consumer reporting agencies. Thus, FCRA protections would not extend to "first parties" that collect information, such as IoT device manufacturers that do in-house analytics. IoT Report at 16.

[44] FED. TRADE COMM'N, CROSS-DEVICE TRACKING (Nov. 2015) (workshop), *available at https://www.ftc.gov/news-events/events-calendar/2015/11/cross-device-tracking*.

percent of those sites collected personally identifiable information from users.[45] Consumers are often unaware of this cross-device tracking, and have limited ability to opt out.[46]

3. Risks to Disadvantaged Communities

The RFC also asks about the impact the Internet of Things might have on disadvantaged or rural communities.[47] As noted above, data generated by IoT devices can support advances in energy, health care, and car safety, among others, and have a beneficial impact on low-income and underserved populations. On the other hand, inaccurate or biased analyses of IoT data can lead to consumers being denied opportunities for education, employment or credit. Companies may seek more data, including IoT data,[48] in order to improve their analysis, but having more data does not necessarily eliminate the risks of inaccuracy or bias. For example, an employment research firm found commuting distance to be one of the strongest predictors of how long a customer service employee will keep a job. But they realized that commuting distance is often correlated with race, and declined to use this predictor out of concern that using it would reduce workplace diversity and potentially violate equal-employment-opportunity standards.[49]

Earlier this year, the FTC issued a report on the impact of big data on underserved consumers, which describes such risks in more detail.[50] One specific challenge is ensuring or compensating for an incomplete data set. For example, Hurricane Sandy generated more than twenty million tweets between October 27 and November 1, 2012. The greatest number of tweets came from Manhattan, creating the illusion that Manhattan was the hub of the disaster. Very few messages originated from more severely affected locations, such as Breezy Point, Coney Island, and Rockaway – areas with lower levels of smartphone ownership and Twitter usage. As

---

[45] *Id.* (Cross Device Tracking Presentation, event materials tab, Slide 33).

[46] *See* Ctr. for Dem. & Tech., *Comments for November 2015 Workshop on Cross-Device Tracking*, at 8 (Oct. 16, 2015), *available at* https://cdt.org/files/2015/10/10.16.15-CDT-Cross-Device-Comments.pdf (indicating that user understanding and transparency around cross-device tracking is very low); Elec. Privacy Info. Ctr, *Comments of The Electronic Privacy Information Center to the Federal Trade Commission, Cross-Device Tracking Workshop*, at 10 (Dec. 16, 2015), *available at* https://www.ftc.gov/policy/public-comments/2015/12/16/comment-00069; and Common Sense Kids Action, *Response Comments to November 2015 Workshop on Cross-Device Tracking*, at 3 (Dec. 16, 2015), *available at* https://www.ftc.gov/policy/public-comments/2015/12/16/comment-00066 (indicating that children and teens are less likely to be aware of cross-device tracking or understand its implications for their futures). Although one self-regulatory organization has released guidance on cross device tracking, that guidance is currently in its implementation period. Another self-regulatory code does apply to cross device tracking, but the opt-out is limited. *See* Network Advertising Initiative, *FAQs on Non-Cookie Technologies* (visited on June 2, 2016), *available at* https://www.networkadvertising.org/code-enforcement/faqs-non-cookie-technologies#3; Digital Advertising Alliance, *Application of the Self-Regulatory Principles of Transparency and Control to Data Used Across Devices*, (Nov. 2015), *available at* http://www.aboutads.info/sites/default/files/DAA_Cross-Device_Guidance-Final.pdf (the opt-out is cookie-based and would apply only to a specific browser or device).

[47] RFC, *supra* note 1 (Question 19).

[48] Transcript of Big Data: A Tool for Inclusion or Exclusion?, in Washington, D.C. (Sept. 15, 2014), at 231-32 (Daniel Castro and Michael Spaeda in conversation).

[49] WHITE HOUSE, BIG DATA: A REPORT ON ALGORITHMIC SYSTEMS, OPPORTUNITY, AND CIVIL RIGHTS, at 15 (May 2016), *available at* https://www.whitehouse.gov/sites/default/files/microsites/ostp/2016_0504_data_discrimination.pdf.

[50] FED. TRADE COMM'N, BIG DATA: A TOOL FOR INCLUSION OR EXCLUSION? UNDERSTANDING THE ISSUES, 27-28 (Jan. 2016) (report), *available at* https://www.ftc.gov/news-events/press-releases/2016/01/ftc-report-provides-recommendations-business-growing-use-big-data [hereinafter Big Data Report].

extended power blackouts drained batteries and limited cellular access, even fewer tweets came from the worst hit areas. If organizations were to base decisions on where to deploy emergency services on this incomplete data set, the people who needed services the most might not have received them.[51]

IV. PRIVACY AND SECURITY RECOMMENDATIONS

Industry and government stakeholders both have an important role to play in fostering innovation in the Internet of Things, while at the same time minimizing privacy and security risks.[52] As NTIA's recent analysis of Census data shows, negative privacy and security experiences can have a direct impact on consumer trust, which could lead to consequences for IoT innovation.[53] This section discusses the respective roles of industry and government in fostering innovation by building consumer trust.

A. Best Practices for Businesses

1. Security

There is widespread consensus that companies developing IoT products and services should implement reasonable security.[54] In creating their security programs, the FTC staff has recommended that, among other things, companies in the IoT space: (1) build security into their devices at the outset; (2) train employees on good security practices; (3) ensure downstream privacy and data protections through vendor contracts and oversight; (4) apply defense-in-depth strategies that offer protections at multiple levels and interfaces; and (5) put in place reasonable access controls.[55] The FTC's *Careful Connections* and *Start with Security* publications offer more detailed guidance.[56]

Staff has also discussed the important role of patching and updating products – particularly in the context of IoT devices. Consumers benefit when companies monitor and patch vulnerabilities throughout the lifecycle of their products. As noted above, in some instances, however, manufacturers of IoT devices might cease technical support and software updates as they release newer versions of the device. In these cases, companies may determine that providing security patches is too costly and may choose not to invest in such patches. Companies should weigh their decisions about software patches carefully against the risk of consumers continuing to use unsupported IoT devices. Many consumers purchase IoT devices with the

---

[51] *Id.*
[52] RFC, *supra* note 1 (Questions 15-19).
[53] Rafi Goldberg, *Lack of Trust in Internet Privacy and Security May Deter Economic and Other Online Activities*, Nat'l Telecomm. & Info. Admin (May 13, 2016) (blog), *available at* https://www.ntia.doc.gov/blog/2016/lack-trust-internet-privacy-and-security-may-deter-economic-and-other-online-activities.
[54] IoT Report at 27.
[55] *Id.* at 27-31. *See also* Fed. Trade Comm'n, *Securing Your Wireless Network* (Sept. 2015), *available at* https://www.consumer.ftc.gov/articles/0013-securing-your-wireless-network.
[56] Careful Connections and Start with Security, *supra* note 10. *See also* Fed. Trade Comm'n, *Securing Your Wireless Network* (Sept. 2015), *available at* https://www.consumer.ftc.gov/articles/0013-securing-your-wireless-network.

expectation that their privacy and security will be protected throughout the life of a product.[57] If this is not the case, companies should truthfully convey to consumers the extent to which they intend to provide security updates to their devices. When feasible, disclosing the length of time companies plan to support and release software updates for a given product line will help consumers better understand the safe "expiration dates" for their Internet-connected devices.[58]

Where an IoT company fails to implement reasonable security, it could be violating the FTC Act's prohibition against deceptive and unfair practices. For example, in its first IoT case, the FTC brought an action against a company, TRENDnet, which sold Internet-connected cameras for purposes ranging from home security to baby monitoring. While advertising their products as secure, the FTC alleged that the company failed to build security into the design of their products, train their employees, implement a process for actively monitoring security vulnerabilities, and perform security tests.[59] In a more recent case against router manufacturer ASUS, the FTC charged that the company failed to reasonably secure the routers it sold to consumers, resulting in vulnerabilities that allowed hackers to gain unauthorized access into thousands of consumers' networks. Among other things, according to the complaint, the company failed to perform security reviews, code review and testing, or vulnerability and penetration testing. The complaint further alleged that the company failed to implement readily-available, low-cost protections against reasonably foreseeable vulnerabilities.[60] Under the proposed order, ASUS must establish a comprehensive security program and notify consumers about software updates or other steps they can take to protect themselves from security flaws.[61]

2. Data Minimization

Data minimization refers to the concept that companies should limit the data they collect and retain, and dispose of it once they no longer need it. Staff recommends that companies in the IoT space should consider reasonable data minimization practices.[62]

Data minimization can help guard against two privacy-related risks. First, larger data stores present a more attractive target for data thieves, both outside and inside a company – and increases the potential harm to consumers from such an event. Second, if a company collects and

---

[57] Chris Ely, *The Life Expectancy of Electronics*, Consumer Technology Association (Sept. 16, 2014), *available at* http://www.cta.tech/Blog/Articles/2014/September/The-Life-Expectancy-of-Electronics.
[58] IoT Report at 31-32.
[59] TRENDnet, Inc., No. C-4426 (Feb. 7, 2014) (complaint), *available at* https://www.ftc.gov/enforcement/cases-proceedings/122-3090/trendnet-inc-matter.
[60] ASUSTeK Computer, Inc., FTC No. 1423156 (Feb. 26, 2016) (complaint), *available at* https://www.ftc.gov/enforcement/cases-proceedings/142-3156/asustek-computer-inc-matter.
[61] *Id.* (proposed consent order).
[62] IoT Report at iv. Commissioner Ohlhausen does not support the data minimization recommendation for the reasons she stated in response to the IoT Report. *See* IoT Report, Separate Statement of Commissioner Maureen K. Ohlhausen at 2 (January 21, 2015) ("[T]he report's support for data minimization embodies what scholar Adam Thierer has called the 'precautionary principle,' and I cannot embrace such an approach. The report, without examining costs or benefits, encourages companies to delete valuable data – primarily to avoid hypothetical future harms. Even though the report recognizes the need for flexibility for companies weighing whether and what data to retain, the recommendation remains overly prescriptive.").

retains large amounts of data, there is an increased risk that the data will be used in a way that departs from consumers' reasonable expectations.[63]

To minimize these risks, companies should examine their data practices and business needs and develop policies and practices that impose reasonable limits on the collection and retention of consumer data. However, recognizing the need to balance future, beneficial uses of data with privacy protection, staff suggests several options for companies to consider. They can decide not to collect data at all; collect only the fields of data necessary to the product or service being offered; collect data that is less sensitive; or deidentify the data they collect.[64] If a company determines that none of these options will fulfill its business goals, it can seek consumers' consent for collecting additional, unexpected categories of data, as explained below.[65]

3. Notice and Choice

Consumer choice continues to play an important role in the IoT. Some stakeholders have suggested that offering notice and choice is challenging in the IoT because of the ubiquity of data collection and the practical obstacles to providing information to consumers when products lack a user interface.[66] However, staff believes that providing notice and choice remains important and practicable in the IoT.[67]

This does not mean that every data collection requires choice. The Commission has recognized that providing choices for every instance of data collection is not necessary to protect privacy and could impose unwarranted burdens on both consumers and businesses. In particular, it has stated that companies should not be compelled to provide choice before collecting and using consumer data for practices that are consistent with the context of a transaction or the company's relationship with the consumer. Indeed, because these data uses are generally consistent with consumers' reasonable expectations, the cost to consumers and businesses of providing notice and choice likely outweighs the benefits.

These principles apply equally to the IoT.[68] For example, suppose a consumer buys a smart oven from ABC Vending, which is connected to an ABC Vending app that allows the consumer to remotely turn the oven on to the setting, "Bake at 400 degrees for one hour." If ABC Vending decides to use the consumer's oven-usage information to improve the sensitivity of its temperature sensor or to recommend another of its products to the consumer, it need not offer the consumer a choice for these uses, which are consistent with its relationship with the consumer. On the other hand, if the oven manufacturer shares a consumer's personal data with, for example, a data broker or an ad network, such sharing would be inconsistent with the context

[63] *Id.*
[64] While de-identification can be challenging in several contexts, appropriately de-identified data sets that are kept securely and accompanied by strong accountability mechanisms, can reduce many privacy risks.
[65] IoT Report at iv.
[66] IoT Report at v and 40.
[67] *Id.*
[68] *Id.*

of the consumer's relationship with the manufacturer, and the company should give the consumer a choice.[69]

Staff acknowledges the practical difficulty of providing choice when there is no consumer interface and recognizes that there is no one-size-fits-all approach. Some options include developing video tutorials, affixing QR codes on devices, and providing choices at the point of sale, within set-up wizards, or in a privacy dashboard. Whatever approach a company decides to take, the privacy choices it offers should be clear and prominent, and not buried within lengthy documents. In addition, companies may want to consider using a combination of approaches.[70]

Some stakeholders have expressed concern that even if companies provide consumers with choices only in those instances where the collection or use is inconsistent with context, such an approach could restrict unexpected new uses of data with potential societal benefits. These stakeholders urge that use limitations be considered as a supplement to, or in lieu of, notice and choice. With a use-based approach, legislators, regulators, self-regulatory bodies, or individual companies would set "permissible" and "impermissible" uses of certain consumer data.[71]

Staff's approach recognizes these concerns and incorporates certain elements of a use-based model. For instance, the idea of choices being keyed to context takes into account how the data will be used: if a use is consistent with the context of the interaction – in other words, it is an expected use – then a company need not offer a choice to the consumer. For uses that would be inconsistent with the context of the interaction (*i.e.*, unexpected), companies should offer clear and conspicuous choices. And certain of the privacy laws the FTC enforces, like FCRA, specifically prohibit certain uses.[72] In addition, if a company collects a consumer's data and de-identifies that data immediately and effectively, it need not offer choices to consumers about this collection.[73]

Staff has concerns, however, about adopting a pure use-based model for the Internet of Things. First, because use-based limitations are not comprehensively articulated in legislation, rules, or widely-adopted codes of conduct, it is unclear who would decide which additional uses are beneficial or harmful. Second, use limitations alone do not address the privacy and security risks created by expansive data collection and retention. For example, collecting vast amounts of data could raise the risk of harm associated with a data breach. Finally, a pure use-based model would not address consumer concerns about the collection of sensitive information, such as Social Security numbers, precise geolocation, financial, children's, or health information.[74]

---

[69] *Id.* at 41.
[70] *Id. See also* FED. TRADE COMM'N, MOBILE PRIVACY DISCLOSURES: BUILDING TRUST THROUGH TRANSPARENCY (Feb. 2013), *available at* https://www.ftc.gov/reports/mobile-privacy-disclosures-building-trust-through-transparency-federal-trade-commission.
[71] *Id.*
[72] 15 U.S.C. § 1681 *et seq.*
[73] IoT Report at vi.
[74] *Id.* at 14 and 44-45.

The establishment of legislative or widely-accepted multistakeholder frameworks could potentially address some of these concerns by designating permitted or prohibited uses. In the absence of consensus on such frameworks, however, the approach set forth here – giving consumers information and choices about their data – continues to be the most viable one for the IoT in the foreseeable future.[75]

4. Big Data

Given the risks associated with big data analytics of IoT products described above, in addition to complying with existing legal requirements,[76] companies should be aware of existing academic research on how certain uses of big data sets may lead to inaccurate or biased results.[77] This research suggests that companies should consider the following when engaging in big data analytics of IoT data:

- Consider whether their data sets are missing information from particular populations and, if they are, take appropriate steps to address this problem.
- Review their data sets and algorithms to ensure that hidden biases do not have an unintended or disparate impact on certain populations.
- Note that, just because big data found a correlation, that does not necessarily mean the correlation is meaningful. As such, companies should consider the risks of using those results, especially where their policies could negatively affect certain populations. It may be worthwhile to have human oversight of data and algorithms when big data tools are used to make important decisions, like ones implicating health, credit, and employment.
- Consider whether ethical considerations advise against or in favor of using big data in certain circumstances. Companies should consider whether they can use big data in ways that advance opportunities for previously underrepresented populations.[78]

B. The Role of Government in Fostering the IoT

Government can play an important role in protecting consumers while supporting innovation in the IoT. For its part, through speeches and other industry and consumer outreach, Congressional testimony, and advocacy comments such as this one, the FTC will continue to promote the best practices described in this comment and its IoT Report. The FTC will also continue to take enforcement action against IoT companies that violate the laws enforced by the FTC.

Staff believes that IoT-specific privacy and data security legislation would be premature at this time. However, the FTC's efforts could be enhanced by appropriate legislation. For this

---

[75] *Id.*

[76] The FTC's Big Data Report highlights laws that might apply to big data, including the FTC Act, Fair Credit Report Act, and equal opportunity laws. *See* Big Data Report at ii-iv.

[77] *See generally* Big Data Report at vi and 5-11. As one example of research on this issue, see Kate Crawford, *The Hidden Biases in Big Data*, Harv. Bus. Rev. (2013), https://hbr.org/2013/04/the-hidden-biases-in-big-data.

[78] Big Data Report at iv-v. *See also* Lesley Fair, *Why Big Data is a Big Deal*, Fed. Trade Comm'n (Jan. 6, 2016) (blog), *available at* https://www.ftc.gov/news-events/blogs/business-blog/2016/01/why-big-data-big-deal.

reason, the FTC has recommended that Congress enact general (as opposed to IoT-specific) security and privacy legislation. First, the FTC continues to support flexible, technology-neutral data security legislation that would strengthen the FTC's enforcement tools and require companies to notify consumers when there is a security breach. The FTC recommends that general data security legislation should protect consumers against unauthorized access to both personal information and device functionality itself. The security risks associated with IoT devices illustrate the importance of these protections. Such legislation is necessary to protect the health and safety of consumers so that, for example, consumers are notified when a door lock or a car's information systems are breached, even if no personal information is taken.[79]

Second, the FTC has called for broad-based, technology-neutral, general privacy legislation.[80] This stems from concerns about the lack of transparency regarding companies' data practices and the lack of meaningful consumer control over their data. These concerns permeate the IoT space, given the ubiquity of information collection, the broad range of uses that the IoT makes possible, the multitude of companies involved in collecting and using information, and the sensitivity of some of the data at issue. General privacy legislation that addresses these issues through greater transparency and choices could help both consumers and businesses by promoting trust in the IoT marketplace.[81]

V. THE ROLE OF INTEROPERABILITY

The RFC asks about the technological challenges in offering interoperability or standardization between IoT devices and platforms. While interoperability and standardization are important mechanisms to addressing technical barriers to adoption, they can also affect innovation and competition in markets for IoT products. As NTIA considers government policy or action to lessen technical barriers to interoperability, staff offers the following observations and recommends that NTIA consider the potential impact of such actions on competition and consumers.

The adoption of standards that allow for the interoperability of consumer devices often promotes and enhances competition in an industry, with direct benefits for consumers. Such standards have long been recognized as one of the engines driving the modern economy.[82] They have made networks, such as the Internet and wireless telecommunications, more valuable by

[79] IoT Report at vii-viii, 49-50.

[80] Commissioner Ohlhausen disagrees with this portion of the staff's recommendation. She believes that the FTC's current Section 5 authority to prohibit unfair and deceptive acts or practices already requires notice and choice for collecting sensitive personally identifiable information and protects against unfair uses of consumer information that cause or are likely to cause substantial harm that the consumer cannot avoid and which is not outweighed by benefits to consumers or to competition. Furthermore, she notes that the FCRA, HIPAA, and other laws already provide additional sector-specific privacy protections. Thus, Commissioner Ohlhausen questions what harms baseline privacy legislation would reach that the FTC's existing authority cannot. *See* Separate Statement of Commissioner Maureen K. Ohlhausen, https://www.ftc.gov/public-statements/2015/01/separate-statement-commissioner-maureen-k-ohlhausen-regarding-internet.

[81] IoT Report at 51-52.

[82] 2007 IP Report at 33.

allowing products to interoperate in a predictable manner.[83] These standards may increase competition by eliminating switching costs for consumers who want to utilize products manufactured by different companies or move their data between services.[84] In the IoT space, interoperability might foster data portability so that, for example, consumers can move their fitness tracker data from one device to another.[85] Under these types of circumstances, interoperability standards can create value for consumers by increasing competition, innovation, product quality, data portability, and choice.[86]

While standardization can offer many procompetitive benefits, however, full realization of these benefits depends on standards being selected "in a nonpartisan manner. . . and in the presence of 'meaningful safeguards' that 'prevent the standard-setting process from being biased by members with economic interests in stifling product competition.'"[87] Standards—particularly in the information technology and telecommunications industries—are often created through a collaborative standard-setting process involving market participants who normally compete against each other.[88] False or misleading representations or other anticompetitive abuse of collaborative standard setting can reduce competition, minimize the role of consumers, and potentially lock-in existing technological approaches to the detriment of innovation and consumers.[89] Thus, to the extent that NTIA considers adopting policies or taking actions to promote interoperability standards, it should consider policies and actions to promote safeguards that support the full realization of these standards' potential benefits.[90]

More generally, widespread adoption of a collaborative standard—even in the presence of meaningful safeguards—may reduce marketplace competition between different technologies. In some settings, marketplace competition among technologies is a potentially superior means of identifying approaches that offer the greatest benefits.[91] In the IoT context, a marketplace with

---

[83] *Id.*

[84] *See* Fed. Trade Comm'n, Prepared Statement of the Fed. Trade Comm'n before the United States Senate Comm. on the Judiciary Subcommittee on Antitrust, Competition Policy and Consumer Rights concerning Standard Essential Patent Disputes and Antitrust Law at 4 (July 30, 2013), *available at* https://www.ftc.gov/sites/default/files/documents/public_statements/prepared-statement-federal-trade-commission-concerning-standard-essential-patent-disputes-and/130730standardessentialpatents.pdf.

[85] *See* INTERNET SOCIETY, INTERNET OF THINGS: AN OVERVIEW, 47 (Oct 2015), *available at* http://www.internetsociety.org/doc/iot-overview.

[86] *See* Fed. Trade Comm'n, Prepared Statement of the Fed. Trade Comm'n before the United States Senate Comm. on the Judiciary concerning Oversight on the Impact on Competition of Exclusion Orders to Enforce Standard Essential Patents at 4 (July 11, 2012), *available at* https://www.ftc.gov/sites/default/files/documents/public_statements/prepared-statement-federal-trade-commission-concerning-oversight-impact-competition-exclusion-orders/120711standardpatents.pdf.

[87] *Broadcom Corp. v. Qualcomm Inc.*, 501 F.3d 297, 309–10 (2007) (quoting *Allied Tube & Conduit Corp. v. Indian Head, Inc.*, 486 U.S. 492, 500 (1988)).

[88] 2007 IP Report at 33-34.

[89] *Id.*

[90] Such safeguards may include policies that "require participants [in the standard-setting process] to disclose the existence of IP rights that may be infringed by the potential users of a standard in development" and that "require [participants] to commit to license any of their IP that is essential to [a] standard on 'reasonable and nondiscriminatory' ('RAND') terms." *2007 IP Report* at 36.

[91] *See* FED. TRADE COMM'N STAFF, ANTICIPATING THE 21ST CENTURY: COMPETITION POLICY IN THE NEW HIGH-TECH, GLOBAL MARKETPLACE 26 (1996) ("Consumers in some industries may be better served by competition among existing technologies, so that competitors' agreement on a standard could be an undesirable elimination of

different and competing technical approaches to interoperability may provide stronger privacy and data security benefits to consumers compared to a marketplace with a single interoperability standard. Further, a marketplace with competing technical approaches would induce firms to innovate to develop interoperability solutions with privacy and data security attributes desired by consumers. When considering standardization and the interoperability of technologies, NTIA should carefully balance the potential benefits and costs to consumers and firms of standardization and competition.

VI. CONCLUSION

Staff hopes that this information, as expanded in greater detail in its 2015 Internet of Things Report, has been of assistance in furthering NTIA's survey of the IoT environment and the impact of IoT devices on the privacy and security of consumers and their devices. The FTC continues to devote substantial resources in this area and looks forward to working with NTIA to foster competition and innovation in the IoT marketplace while protecting consumers.

---

product variety. In other industries, especially those characterized by the demand-side scale economies associated with network externalities, consumers may benefit from the presence of a single compatible technology.").