Before the

Department of Commerce

National Telecommunications and Information Administration

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 Electronic Frontier Foundation

May 23, 2016

Submitted by:

Corynne McSherry
Jennifer Lynch
Jamie Williams
Electronic Frontier Foundation
815 Eddy Street
San Francisco, CA 94109
Telephone: (415) 436-9333
corynne@eff.org

The Electronic Frontier Foundation (EFF) submits the following comments primarily in response to Question 15 of the National Telecommunications and Information Administration's (NTIA) notice and request for public comment: "What are the main policy issues that affect or are affected by IoT?"

EFF is a member-supported, nonprofit, public interest organization dedicated to protecting privacy, civil liberties and innovation in the digital age. Founded in 1990, EFF represents tens of thousands of dues-paying members, including consumers, hobbyists, computer programmers, entrepreneurs, students, teachers, and researchers. EFF and its members are united in their commitment to ensuring that new technologies are not used to undermine privacy and security, and in their desire for a balanced copyright system that provides adequate incentives for creators, facilitates innovation, and ensures broad access to information in the digital age.

EFF recognizes, just as NTIA recognized in its call for comments, that the Internet of Things (IoT) is one of the fasting-growing technological trends of our day, with the potential to transform the lives of individuals around the world. But it also presents

serious and complex challenges. We focus our comments here on three interrelated challenges in particular: security, privacy, and copyright. Further, although the IoT is much broader than devices collecting data on consumers,[1] our comments here focus on the consumer sector.

I. Risks to Security and Privacy

The FTC has described the IoT as "an interconnected environment where all manner of objects have a digital presence and the ability to communicate with other objects and people."[2] Consumer devices that are and will become part of the Internet of Things are designed to collect data on a near-constant basis and share that data broadly—not only with the consumer, but with other devices, with social media, with the manufacturer, with data aggregators, and with known and unknown third parties. In fact, a recent Hewlett Packard study found that 90 percent of IoT devices collected at least one piece of personal information via the device, the cloud, or its mobile application.[3] This treasure trove of data will prove irresistible for marketers, hackers, law enforcement, and insurance companies. Thus, its collection presents serious risks to security and privacy—at both the individual and societal level.

A. Data Collected and Shared by IoT Devices Will Reveal Intimate and Private Details about Americans' Lives

IoT devices pose threats to privacy not only from the data each individual device collects, but also from the aggregation of that data over time and across devices, and from the sharing of that data with third parties. Already, IoT devices can reveal how we slept last night, how much coffee we had at breakfast, and when we left the house in the morning.[4]

---

[1] The research firm Gartner has predicted there will be 20.8 billion interconnected devices in use by 2020. Of that total, approximately 7.2 billion will be in use by businesses for manufacturing and industry. Gartner, *Gartner Says 6.4 Billion Connected "Things" Will Be in Use in 2016, Up 30 Percent From 2015* (Nov. 10, 2015), https://www.gartner.com/newsroom/id/3165317.

[2] FTC Staff Report, *Internet of Things: Privacy & Security in an Interconnected World* (Jan. 2015), https://www.ftc.gov/system/files/documents/reports/federal-trade-commission-staff-report-november-2013-workshop-entitled-internet-things-privacy/150127iotrpt.pdf.

[3] Hewlett Packard Enterprise, *Internet of Things Research Study: 2015 Report* (2015), http://www8.hp.com/h20195/V2/GetPDF.aspx/4AA5-4759ENW.pdf.

[4] Fitbit, *In-Depth Analysis of Your Sleep*, https://www.fitbit.com/premium/reports/sleep; Justin Yu, *This Quirky smart coffee maker refills its own beans from Amazon's Dash Replenishment Service*, CNet (Apr. 1, 2015), http://www.cnet.com/products/poppy-pour-over/; Nest, *Learn how Auto-Away works on the Nest Thermostat,* https://nest.com/support/article/What-is-Auto-Away.

But when this data is collected over time and shared with other devices, it is also possible to track habits (did we leave the same time as yesterday? As last week? As last year?) and infer lifestyle changes (if we suddenly start leaving earlier, is it because we've changed jobs? started working out more?). It also becomes possible to infer much more personal information, such as relationship status and even sexual habits.[5]

Moreover, as data on multiple people are collected, aggregated, and compared, companies can determine information about communities as a whole—such as how an earthquake is felt around the Bay Area, which neighborhoods use the most energy, and who is responsible for traffic problems in the morning commute.[6] This kind of monitoring will only increase in the future, as IoT devices become an even greater part of our daily lives, whether woven into our clothing to detect and regulate body heat or built into our plates to determine how much we eat.[7] As a director at Siemens has described this issue in regard to their smart meters, the "masses of private data" collected by IoT devices can allow a company to "infer how many people are in the home, what they do, whether they are upstairs, downstairs, do you have a dog, when do you usually get up, when did you get up this morning, when you have a shower."[8]

IoT devices may also collect sensitive and private information in ways we wouldn't suspect. In 2015, we learned that Samsung Smart TV's voice command feature also allowed its televisions to capture viewers' private conversations and potentially share those conversations with third parties.[9] While Samsung appears to have modified this feature such that it now requires explicit viewer activation, without proper security

---

[5] Leena Rao, *Sexual Activity Tracked By Fitbit Shows Up In Google Search Results,* TechCrunch (July 3, 2011), http://techcrunch.com/2011/07/03/sexual-activity-tracked-by-fitbit-shows-up-in-google-search-results/.

[6] Eugene Mandel, *How the Napa Earthquake affected Bay Area sleepers*, The Jawbone Blog (Aug 25, 2014), https://jawbone.com/blog/napa-earthquake-effect-on-sleep/.

[7] Christian de Looper, *Top 5 Internet Of Things Devices To Expect In The Future*, Tech Times (Feb. 8, 2015), http://www.techtimes.com/articles/31467/20150208/top-5-internet-things-devices-expect-future.htm; *About the Nest Home Report*, https://nest.com/support/article/About-the-Nest-Home-Report Pu Wang, et al. "Understanding Road Usage Patterns in Urban Areas," Nature Scientific Reports 2, Article No: 1001 (2012) http://www.nature.com/articles/srep01001.

[8] Brian Fung, *Here's the scariest part about the Internet of Things*, Washington Post (Nov. 19, 2013), https://www.washingtonpost.com/blogs/the-switch/wp/2013/11/19/here's-the-scariest-part-about-the-internet-of-things.

[9] John Ribeiro, *Smart TV eavesdropping furor prompts Senator to quiz Samsung, LG on privacy*, PC World (Feb. 12, 2015), http://www.pcworld.com/article/2883532/us-senator-quizzes-samsung-lg-on-smart-tv-privacy.html.

practices in place, such a feature could be turned on remotely—without the owner's consent or even knowledge—subjecting the owner to repeated invasions of privacy.[10]

Privacy is a top concern for consumers. According to a recent Pew Research Center poll, 91 percent of adults surveyed believe that "consumers have lost control over how personal information is collected and used by companies."[11] Sixty-four percent of those polled "believe the government should do more to regulate advertisers," and few believe companies can be trusted to "do the right thing" on their own.[12]

Although the IoT is still relatively new, consumers are already worried about privacy and security issues posed by the IoT, and this is impacting their spending on IoT devices.[13] Privacy is one of the biggest reasons why consumers who know about in-home IoT devices haven't purchased them.[14] Further, fifty-seven percent of consumers said they are less likely to purchase wearable technology because of hacks and data breaches that have plagued retailers like Target and Home Depot.[15]

Unfortunately, there is insufficient legal protection for privacy in data gathered by IoT devices, either at the state or federal level. This creates an opportunity for NTIA to recommend standards for how companies should collect, retain, protect, and share data gathered by IoT devices. We urge the NTIA to consult with public interest organizations dedicated to protecting consumer privacy and security in formulating such standards.

---

[10] Samsung, *Samsung Smart TVs Do Not Monitor Living Room Conversations* (Feb. 10, 2015), https://news.samsung.com/global/samsung-smart-tvs-do-not-monitor-living-room-conversations; Associated Press, *Will the Internet listen to your private conversations?* (July 29, 2015), http://nypost.com/2015/07/29/will-the-internet-listen-to-your-private-conversations/.

[11] Pew Research Center, *Public Perceptions of Privacy and Security in the Post-Snowden Era*, at 3 (Nov. 12, 2014), http://www.pewinternet.org/files/2014/11/PI_PublicPerceptionsofPrivacy_111214.pdf.

[12] *Id.* at 3, 29.

[13] Altimeter Group, *Consumer Perceptions of Privacy in The Internet of Things* (2015), http://www.altimetergroup.com/2015/06/new-report-consumer-perceptions-of-privacy-in-the-internet-of-things/.

[14] Acquity Group, *The Internet of Things: The Future of Consumer Adoption*, at 6 (2014), http://quantifiedself.com/docs/acquitygroup-2014.pdf.

[15] *Id.* This is consistent with other polls that have shown consumers are concerned about the data collected and shared by smartphones and have taken concrete steps to protect their privacy by deleting or not installing apps they do not trust. *See* Jan Lauren Boyles *et al.*, *Privacy and Data Management on Mobile Devices*, Pew Research Internet & American Life Project (Sept. 5, 2012), http://www.pewinternet.org/2012/09/05/privacy-and-data-management-on-mobile-devices/.

B. The Prevalence of IoT Devices, the Low Cost of Development, and the Massive Data Collection Discussed Above Will Threaten the Security of Consumers' Data

While manufacturers of more expensive consumer-level IoT devices such as wearables have taken steps to develop their products with data security and privacy in mind, many manufacturers have not. For example, mature manufacturers of devices—like appliances that never collected consumer data in the past—likely have little to no experience collecting, securing, and protecting consumer data. And start-ups building IoT technologies and interfaces for the first time may focus solely on a product's capabilities without considering how to protect and secure computer networks or data.

In addition, because manufacturers believe these devices must stay low in cost (such as "smart" light bulbs or sensors in clothing) to compete in the market, manufacturers often use low capability hardware, fail to institute good security protocols, and neglect to send (or by design have no means of sending) critical security updates to consumers—which would be pushed out in the case of a more expensive device, such as a smart phone or computer. This has led a Princeton University professor and doctoral student to rename the IoT phenomenon "The Internet of Unpatched Things."[16] Unpatched smart devices create security vulnerabilities and can put privacy at risk by making devices easier to compromise or by leaking user information.

A study issued by Hewlett-Packard's security research team in November 2015 found that 60 percent of the most commonly used Internet of Things devices had serious security vulnerabilities. The vulnerabilities they discovered through their assessment of the top ten devices then in use revealed privacy issues, lack of transport encryption, insecure web interface, inadequate software protection, and insufficient authorization.[17] To date, there have been countless news stories regarding hacked IoT devices, including not only in-home devices such thermostats and baby monitors[18] but also medical devices (such as insulin pumps, pacemakers, and even hospital equipment[19]), smart vehicles,[20]

---

[16] Sarthak Grover & Nick Feamster, *The Internet of Unpatched Things*, Privacy Con 2016 Presentation Slides, available at https://www.ftc.gov/system/files/documents/public_comments/2015/10/00071-98118.pdf.

[17] *See supra* n. 3, 2015 Hewlett Packard Internet of Things Research Study.

[18] *See* Lily Hay Newman, *Pretty Much Every Smart Home Device You Can Think of Has Been Hacked*, Slate (Dec. 30, 2014), http://www.slate.com/blogs/future_tense/2014/12/30/the_internet_of_things_is_a_long_way_from_being_secure.html.

[19] *See* Kim Zetter, *It's Insanely Easy to Hack Hospital Equipment,* Wired (Apr. 25, 2014), https://www.wired.com/2014/04/hospital-equipment-vulnerable/.

[20] *See* Andy Greenberg, *Hackers Remotely Kill a Jeep on the Highway—With Me in It*, Wired (Jul. 21, 2015), https://www.wired.com/2015/07/hackers-remotely-kill-jeep-highway/.

and the maker of smart-grid control software.[21] These incidents raise not only privacy concerns, given the sensitivity of the data collected, but also serious public safety concerns.

II. Technological and Legal Barriers to Risk Mitigation

To date, most of the security research in the field has come in the form of unstructured privacy and safety evaluations conducted by security researchers or so-called "hackers" at the back end,[22] rather than through manufacturers at the front end.

This suggests that one of the most basic ways to protect the public from the risks outlined above is to ensure that both security researchers and users themselves have the right to test the software embedded in their devices for security flaws—and to determine what information is being collected and how that information is being handled. Unfortunately, a web of technological and legal restrictions impede this necessary research.

A. Para-Copyright Restrictions Inhibit Security Research, Further Threatening Consumer Privacy and Security

Embedded software often includes a technological protection measure (TPM) designed to prevent unauthorized users from freely accessing and/or modifying it. These restrictions may be well intentioned, such as a TPM designed to protect the security of the software so that it cannot be modified in a way that would be harmful to the user. But TPMs can have unexpected consequences. Specifically, researchers may need to circumvent them in order to test the software for security or privacy flaws.

As a technical matter, such circumvention is usually easy to do. Unfortunately, it also comes with significant legal risk, thanks to Section 1201 of the Digital Millennium Copyright Act (DMCA).

Section 1201 contains two distinct prohibitions: (i) a ban on acts of circumvention; and (ii) a ban on the distribution of tools and technologies used for circumvention. The "act" prohibition, set out in section 1201(a)(1), prohibits the act of circumventing a technological measure used by copyright owners to control access to their works (*i.e.*, "access controls"). The ban applies even where the purpose for decrypting the movie would otherwise be legitimate. The "tools" prohibitions, set out in sections 1201(a)(2) and 1201(b), outlaw the manufacturing, sale, distribution, or trafficking of tools and technologies that make circumvention possible.

---

[21] *See* Kim Zetter, *Maker Of Smart-Grid Control Software Hacked*, Wired (Sep. 26, 2012), https://www.wired.com/2012/09/scada-vendor-telvent-hacked/.

[22] *See, e.g.*, Kelly Jackson Higgins, *Hiring Hackers To Secure The Internet Of Things*, Dark Reading (Dec. 11, 2014), http://www.darkreading.com/vulnerabilities%E2%80%94-threats/hiring-hackers-to-secure-the-internet-of-things/d/d-id/1318107.

Section 1201 includes a number of exceptions for certain limited classes of activities, including security testing, reverse engineering of software, encryption research, and law enforcement, but these exceptions are often too narrow to be of use to the constituencies they were intended to assist.[23] As Professor Edward Felten has put it, the security research exceptions "appear[] to have been written without consulting any researchers."[24]

Section 1201 has only minimal effect as a means of preventing copyright infringement, because copyright infringement is itself illegal and carries substantial civil and sometimes criminal penalties.[25] One who risks actual or statutory damages, injunctive relief, seizure of materials and equipment, and attorney fee awards is not likely to be deterred any more strongly by the possibility of similar remedies for circumvention.

Unfortunately, however, Section 1201 has been an effective means of stifling free speech and legitimate scientific research. The threat was illustrated early on by the actions of the multi-industry group Secure Digital Music Initiative (SDMI), which issued a public challenge encouraging skilled technologists to try to defeat certain watermarking technologies intended to protect digital music. Professor Felten and a team of researchers at Princeton, Rice, and Xerox took up the challenge and succeeded in removing the watermarks. But when the team tried to present their results at an academic conference, SDMI representatives threatened the researchers with liability under the DMCA. The researchers ultimately withdrew their paper from the conference. Although SDMI withdrew the threat after the researchers took the matter to court, at least one of the researchers involved decided to forgo further research efforts in the field as a result of his experience.[26]

Threats like this have chilled legitimate activities of journalists, publishers, scientists, students, programmers, and others. Bowing to fears of DMCA liability, online service providers have censored discussions of copy-protection systems, programmers have

---

[23] *See* Pamela Samuelson, *Intellectual Property and the Digital Economy: Why the Anti-Circumvention Regulations Need to be Revised*, 14 Berkeley Law Journal 519, 537-57 (1999).

[24] *See* Edward Felten, *The Chilling Effects of the DMCA*, Slate (Mar. 29, 2013), http://www.slate.com/articles/technology/future_tense/2013/03/dmca_chilling_effects_how_copyright_law_hurts_security_research.single.html.

[25] *See* 17 U.S.C. § 106, 501–506*; see also* Pamela Samuelson and Tara Wheatland, *Statutory Damages in Copyright Law: A Remedy In Need of Reform*, 51 Wm. & Mary L. Rev. 439 (2009).

[26] Pamela Samuelson, *Anticircumvention Rules: Threat to Science*, 293 Science 2028, (Sept. 14, 2001); Letter from Matthew Oppenheim, SDMI General Counsel, to Prof. Edward Felten (Apr. 9, 2001), http://cryptome.org/sdmi-attack.htm; EFF, *Felten, et al. v. RIAA, et al.* Case Page, https://www.eff.org/cases/felten-et-al-v-riaa-et-al.

removed computer security programs from their websites, and students and security experts have stopped publishing details of their research.[27]

The DMCA does provide for a triennial rulemaking that was meant as a "fail-safe" to prevent its provisions from encroaching on the public's ability to engage in activities that would otherwise be perfectly legal under copyright law. Unfortunately, the rulemaking has not served its purpose. The exemptions created by the Copyright Office are too narrow and too brief—and to date they have not effectively been able to protect the rights of security researchers and users to test the security of their devices.

These developments weaken security for all computer users—including, ironically, copyright owners counting on technical measures to protect their works. They also threaten the security of all IoT devices. In the interest of protecting security in the age of the Internet of Things, NTIA should be deeply concerned about any legal restriction that could inhibit researchers' and users' ability to find and publicize security vulnerabilities.

To ensure that the DMCA doesn't impede security and privacy research and testing in the age of the Internet of Things, NTIA, as the President's principal adviser on telecommunications and information policy, should recommend that Congress overturn Section 1201 altogether. Short of that, the law should be scaled back to ensure that its applicability is limited to the situations it was intended to target: using or distributing tools for circumvention should not be a violation unless the use or distribution is intended to facilitate copyright infringement. Not only would this bring the law back in line with its intent, but it would ensure the both security researches and users' alike have the ability to test the security of their devices—to the benefit of the public.

In the meantime, NTIA should take advantage of its special consulting role in the triennial rulemaking process to recommend that the Librarian undertake the following reforms:

- *Independent Fact-Finding.* As part of the triennial rulemaking, the Copyright Office should actively solicit input from users and undertake independent fact-finding to determine whether lawful uses of copyrighted works are being impaired by TPMs.

- *Reduce Complexity and Re-assign Burdens of Proof.* Once a petitioner comes forward with a concern regarding a lawful use that appears to be impaired by DRM restrictions, the burden should then shift to the copyright owner to (1) describe how the TPM functions and how widely it is deployed; and (2) demonstrate by a preponderance of the evidence that continuing DMCA protection is necessary to the market viability of the work.

---

[27] *See* EFF, *Unintended Consequences: Sixteen Years Under the DMCA* (Sep. 2014), https://www.eff.org/files/2014/09/16/unintendedconsequences2014.pdf.

- *Leave Fair Use to the Courts*. Where a petitioner comes forward with a use, otherwise impeded by TPM restrictions, that might plausibly be viewed by a court as a fair use, the Copyright Office should presume that the use in question is a fair use for purposes of considering whether an exemption should be granted.

B. Contract Restrictions Also Inhibit Security Research

Non-negotiated contracts of adhesion attached to the software embedded in user devices—which commonly take the form of End User License Agreements (EULAs) or Terms of Service (ToS)—also threaten the security of IoT devices and, subsequently, the privacy of user data.

Rightsholders commonly use such "contracts" to not only prevent the resale or lending of copyrighted works and software-enabled devices, but also to prevent fair uses, including reverse engineering that is often necessary for security research and testing. Moreover, companies that present a wall of legalese to their users (or put that legalese online), knowing it will almost always go unread—unless and until the vendor chooses to enforce the contract.

A recent study shows that the majority of Americans feel that their rights are abused by software-enabled services but feel powerless to stop it.[28] That perception is well-founded. Because most such contracts of adhesion mandate arbitration, it is difficult if not impossible for consumers to meaningfully challenge unfair terms.

Neither can market forces remedy these abuses for several reasons. First, the inquiry a purchaser would need to make to decide between different products' terms is prohibitive—even without hiring a lawyer. Second, the abusive terms documented below are widespread and many products are unique, meaning that alternatives are not available. Finally, because purchasers do not read EULAs and terms of service, they are not aware of particular abusive terms that might prompt them to seek alternatives, until it is too late.

Accordingly, the NTIA should recommend that the President commission a study focusing specifically on the EULA problem, and develop practical recommendations that could serve as a basis for state or federal legislation. Those recommendations could include:

- *Limits on liability*. A party who agrees not to reverse engineer, and does so anyway, may be liable for breach of contract, but should not be subjected to the punitive sledgehammer of copyright's statutory damages. Just as a

---

[28] Joseph Turow, Michael Hennessey, and Nora Draper, *The Tradeoff Fallacy: How Marketers are Misrepresenting American Consumers and Opening Them Up to Exploitation*, Annenberg School for Communication, U. Penn. 3 (2015), https://www.asc.upenn.edu/sites/default/files/TradeoffFallacy_1.pdf.

copyright term having nothing to do with copyright law should not create infringement liability, neither should contract terms that purport to erase rights explicitly preserved by copyright law (such as fair use rights to reverse engineer).[29]

- *User rights under copyright law should not be waived by adhesive terms or "magic words."* Copyright law contains a number of protections for the owner of a copy of a work, which protect freedom of speech, personal autonomy, competition, and innovation. Some courts have made clear that transaction resembling a sale cannot be transformed into a mere license via the recitation of magic words. The Second Circuit explained in *Krause* that, regardless of the formalities of transfer, a purchaser of a copy of a copyrighted work can exercise the rights of a copy owner as long as their possession involves "sufficient incidents of ownership" over the copy, such as payment of consideration, the right to use or discard the copy, and ownership of the tangible property on which the work resides.

- *Contract restrictions should be transparent to users, prior to purchase*. Contracts governing the sale of devices with embedded software that include clauses that will impede security and privacy research should include clear warnings to the purchaser, prior to purchase, on the product's packaging or marketing materials. Such warnings should explicitly identify, in simple language, the effect of the waiver.

We note that the Copyright Office is also studying the specific issue of embedded software. This additional study could complement that effort by exploring options for reform that focus on contract restrictions that inhibit security and privacy research.

---

[29] The Ninth Circuit has begun to address this problem by holding that contractual covenants having no nexus to copyright law cannot be converted into copyright violations by characterizing them as limits on a license. The court observed that allowing a software copyright holder to "designate any disfavored conduct during software use as copyright infringement . . . would allow software copyright owners far greater rights than Congress has generally conferred on copyright owners." *MDY Indus., LLC v. Blizzard Entm't, Inc*., 629 F.3d 928, 941 (9th Cir. 2010), *as amended on denial of reh'g* (Feb. 17, 2011), *opinion amended and superseded on denial of reh'g,* No. 09-15932, 2011 WL 538748 (9th Cir. Feb. 17, 2011).

III. Conclusion

To ensure that the risks presents by the Internet of Things do not overpower its potential benefits, the security and privacy of those things must be subject to regular scrutiny. That scrutiny, in turn, depends in turn on removing barriers to that scrutiny. NTIA should highlight these three interrelated issues in its "green paper" and recommend that the President push for substantial reforms to protect consumer privacy and security. NTIA should also work with the privacy community to establish standards for how companies should collect, retain, protect, and share data gathered by IoT devices, and NTIA should remain transparent throughout that process.

Respectfully submitted,

Corynne McSherry
Jennifer Lynch
Jamie Williams
Electronic Frontier Foundation
815 Eddy Street
San Francisco, CA 94109
Telephone: (415) 436-9333
corynne@eff.org