epic.org

Electronic Privacy Information Center
1718 Connecticut Avenue NW, Suite 200
Washington, DC 20009, USA

+1 202 483 1140
+1 202 483 1248
@EPICPrivacy
https://epic.org

October 2, 2017

The Honorable William Hurd, Chairman
The Honorable Robin Kelly, Ranking Member
U.S. House Committee on Oversight and Government Reform
Subcommittee on Information Technology
2157 Rayburn House Office Building
Washington, DC 20515

RE: "Cybersecurity of the Internet of Things"

Dear Chairman Hurd and Ranking Member Kelly:

We write to you regarding the "Cybersecurity of the Internet of Things" hearing.[1] American consumers face unprecedented privacy and security threats. The unregulated collection of personal data and the growth of the Internet of Things has led to staggering increases in identity theft, security breaches, and financial fraud in the United States. These issues have a significant impact on the future of cybersecurity, and we commend the Subcommittee for exploring them. Congress should develop meaningful safeguards for the privacy and security of Americans' health information.

EPIC is a public interest research center established in 1994 to focus public attention on emerging privacy and civil liberties issues.[2] EPIC is a leading advocate for consumer privacy, and has actively participated in the proceedings of the Federal Trade Commission ("FTC") and the Federal Communications Commission ("FCC").[3]

---

[1] *Cybersecurity of the Internet of Things*, 115th Cong. (2017), H. Comm. on Oversight and Gov't Reform, Subcomm. on Information Technology, https://oversight.house.gov/hearing/cybersecurity-internet-things/ (October 3, 2017).

[2] *See* EPIC, *About EPIC*, https://epic.org/epic/about.html.

[3] *See, e.g,* Marc Rotenberg, EPIC Executive Director, Testimony before the U.S. House Energy & Commerce Subcommittee on Communications and Technology, *Examining the EU Safe Harbor Decision and Impacts for Transatlantic Data Flows* (November 13, 2015), https://epic.org/privacy/intl/schrems/EPIC-EU-SH-Testimony-HCEC-11-3-final.pdf; Marc Rotenberg, EPIC Executive Director, Testimony before the U.S. House Energy & Commerce Subcommittee on Communications and Technology, *Communications Networks and Consumer Privacy: Recent Developments* (April 23, 2009), https://epic.org/privacy/dpi/rotenberg_HouseCom_4-09.pdf; Letter from EPIC to the U.S. House Committee on Energy and Commerce on FCC Privacy Rules (June 13, 2016), https://epic.org/privacy/consumer/EPIC-FCC-Privacy-Rules.pdf; Letter from EPIC to the U.S. Senate Committee on Commerce, Science, and Transportation on FTC Oversight (Sept. 26, 2016), https://epic.org/privacy/consumer/EPIC-Letter-Sen-Comm-CST-FTC-Oversight.pdf.

The Internet of Things Poses Numerous Privacy and Security Risks

The Internet of Things (IoT) poses significant privacy and security risks to American consumers.[4] The Internet of Things expands the ubiquitous collection of consumer data. This vast quantity of data could be used for purposes that are adverse to consumers, including remote surveillance. Smart devices also reveal a wealth of personal information about consumers, which companies may attempt to exploit by using it to target advertising or selling it directly. Because the IoT generates data from all aspects of consumers' daily existence, these types of secondary uses could lead to the commercialization of intimate segments of consumers' lives.

Many IoT devices feature "always on" tracking technology that surreptitiously records consumers' private conversations in their homes.[5] These "always on" devices raise numerous privacy concerns, including whether consumers have granted informed consent to this form of tracking. Even if the owner of an "always on" device has consented to constant, surreptitious tracking, a visitor to their home may not. Companies say that the devices rely on key words, but to detect those words, the devices must always be listening. And the key words are easily triggered. For example, several Amazon Echo devices treated a radio broadcast about the device as commands.[6] A San Diego television report about a girl using an Echo to order a $170 dollhouse and four pounds of sugar cookies triggered Echo devices across the city to make the same purchase.[7] A recent law enforcement request for Amazon Echo recordings[8] shows that "always on" devices will be much sought-after sources of information by law enforcement, foreign and domestic intelligence agencies, and, inevitably, cybercriminals.

Another significant risk to consumers in the IoT is security, of both the users' data and their physical person. Many of the same security risks that currently threaten our data will only expand in the Internet of Things. The damage caused by malware, phishing, spam, and viruses will have an increasingly large array of networks in which to spread.[9] Additionally, not all wireless connections in the IoT are encrypted.[10] Researchers who studied encryption within the

---

[4] *See* Comments of EPIC to NTIA, *On the Benefits, Challenges, and Potential Roles for the Government in Fostering the Advancement of the Internet of Things* (June 2, 2016), https://epic.org/apa/comments/EPIC-NTIA-on-IOT.pdf; *Internet of Things,* EPIC, https://epic.org/privacy/internet/iot/.

[5] EPIC Letter to DOJ Attorney General Loretta Lynch, FTC Chairwoman Edith Ramirez on "Always On" Devices (July 10, 2015), https://epic.org/privacy/internet/ftc/EPIC-Letter-FTC- AG-Always-On.pdf.

[6] Rachel Martin, *Listen Up: Your AI Assistant Goes Crazy For NPR Too*, NPR (Mar. 6, 2016), http://www.npr.org/2016/03/06/469383361/listen-up-your-ai-assistant-goes-crazy-for-npr-too.

[7] Carlos Correa, *News Anchor Sets off Alexa Devices Around San Diego Ordering Unwanted Dollhouses*, CW6 (Jan. 5, 2017), http://www.cw6sandiego.com/news-anchor-sets-off-alexa- devices-around-san-diego-ordering-unwanted-dollhouses/.

[8] *See* Christopher Mele, *Bid for Access to Amazon Echo Audio in Murder Case Raises Privacy Concerns*, N.Y. Times (Dec. 28, 2016), https://www.nytimes.com/2016/12/28/business/amazon- echo-murder-case-arkansas.html.

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

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

IoT found that "many of the devices exchanged personal or private information with servers on the Internet in the clear, completely unencrypted."[11]

In addition to data security risks, the IoT also poses risks to physical safety and personal property. This is particularly true given that the constant flow of data so easily delineates sensitive behavior patterns, and flows over networks that are not always secure, leaving consumers vulnerable to malicious hackers. For instance, a hacker could monitor Smart Grid power usage to determine when a consumer is at work, facilitating burglary, unauthorized entry, or worse. Researchers have already demonstrated the ability to hack into connected cars and control their operation, which poses potentially catastrophic risks to the public.[12]

It is not only the owners of IoT devices who suffer from the devices' poor security. The IoT has become a "botnet of things"—a massive network of compromised web cameras, digital video recorders, home routers, and other "smart devices" controlled by cybercriminals who use the botnet to take down web sites by overwhelming the sites with traffic from compromised devices.[13] The IoT was largely to blame for attacks in 2016 that knocked Twitter, Paypal, Reddit, Pinterest, and other popular websites off of the web for most of a day.[14] They were also behind the attack on security blogger Brian Krebs' web site, one of the largest attacks ever seen.[15]

These problems will not be solved by the market. Because poor IoT security is something that primarily affects other people, neither the manufacturers nor the owners of those devices have any incentive to fix weak security. Compromised devices still work fine, so most owners of devices that have been pulled into the "botnet of things" had no idea that their IP cameras, DVRs, and home routers are no longer under their own control. As Bruce Schneier said in recent congressional testimony, a manufacturer who puts a sticker on the box that says "This device costs $20 more and is 30 percent less likely to annoy people you don't know" probably will not get many sales.[16]

---

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

[12] *See, e.g.*, Karl Brauer & Akshay Anand, *Braking the Connected Car: The Future of Vehicle Vulnerabilities*, RSA Conference 2016, https://www.rsaconference.com/writable/presentations/file_upload/ht-t11-hacking-the-connected-car-thetfuturetof-vehicle-vulnerabilities.pdf ; FireEye, *Connected Cars: The Open Road for Hackers* (2016), https://www.fireeye.com/content/dam/fireeye-www/services/pdfs/connected-cars-the-open-road-for-hackers.pdf.

[13] *See* Bruce Schneier, *We Need to Save the Internet from the Internet of Things*, Schneier on Security (Oct. 6, 2016), https://www.schneier.com/essays/archives/2016/10/we_need_to_save_the_.html

[14] *See* Scott Hilton, *Dyn Analysis Summary of Friday October 21 Attack*, Dyn.com (Oct. 26, 2016), http://dyn.com/blog/dyn-analysis-summary-of-friday-october-21-attack/.

[15] *See* Brian Krebs, *KrebsOnSecurity Hit With Record DDoS*, KrebsOnSecurity (Sept. 21, 2016), https://krebsonsecurity.com/2016/09/krebsonsecurity-hit-with-record-ddos/.

[16] Testimony of Bruce Schneier before the House Committee on Energy & Commerce, Understanding the Role of Connected Devices in Recent Cyber Attacks, 114th Cong. (2016).

We ask that this letter be entered in the hearing record. EPIC looks forward to working with the Subcommittee on these and other issues impacting the privacy and security of American consumers.

Sincerely,

/s/ *Marc Rotenberg*
Marc Rotenberg
EPIC President

/s/ *Caitriona Fitzgerald*
Caitriona Fitzgerald
EPIC Policy Director