epic.org | ELECTRONIC PRIVACY INFORMATION CENTER

January 23, 2017

The Honorable John Thune, Chairman
The Honorable Bill Nelson, Ranking Member
U.S. Senate Committee on Commerce, Science, and Transportation
Dirksen Senate Building, Room 512
Washington, DC 20510

RE: Markup of S. 88, Developing Innovation and Growing the Internet of Things (DIGIT) Act, and S. 134, Spoofing Prevention Act

Dear Chairman Thune and Ranking Member Nelson:

The Electronic Privacy Information Center ("EPIC") writes to you regarding the upcoming executive session to consider S. 88, Developing Innovation and Growing the Internet of Things ("DIGIT") Act, and S. 134, Spoofing Prevention Act. American consumers are concerned about the risks of connected devices. EPIC supports legislation that safeguards consumer privacy and promotes public safety. We are not satisfied that these pending measures adequately address the concerns of American consumers.

The Internet of Things Poses Numerous Privacy and Security Risks

The Internet of Things poses significant privacy and security risks to American consumers.[1] 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 Internet of Things 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 Internet of Things devices feature "always on" tracking technology that surreptitiously records consumers' private conversations in their homes.[2] These "always on" devices raise numerous privacy concerns, including whether consumers have granted informed

[1] *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; EPIC, *Internet of Things*, https://epic.org/privacy/internet/iot/.
[2] 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.

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 in order to detect those words, the devices must be listening at all times. And the key words are easily triggered. For example, several Amazon Echo devices treated a radio broadcast about the device as commands.[3] 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.[4] A recent law enforcement request for Amazon Echo recordings[5] 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 Internet of Things is security, of both the users' data and their physical person. Many of the same security risks that currently threaten our data will only expand in the Internet of Things. The damage caused by malware, phishing, spam, and viruses will have an increasingly large array of networks in which to spread.[6] Additionally, not all wireless connections in the Internet of Things are encrypted.[7] Researchers who studied encryption within the Internet of Things found that "many of the devices exchanged personal or private information with servers on the Internet *in the clear*, completely unencrypted."[8]

In addition to data security risks, the Internet of Things also poses risks to physical safety and personal property. This is particularly true given that the constant flow of data so easily delineates sensitive behavior patterns, and flows over networks that are not always secure, leaving consumers vulnerable to malicious hackers. 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.[9]

---

[3] 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.
[4] 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/.
[5] *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.
[6] *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
[7] 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.
[8] 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).
[9] *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*

It is not only the owners of Internet of Things devices who suffer from the devices' poor security. The Internet of Things 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.[10] The Internet of Things 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.[11] They were also behind the attack on security blogger Brian Krebs' web site, one of the largest attacks ever seen.[12]

These problems will not be solved by the market. Because poor Internet of Things 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" have 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.[13] We urge the Committee to address these numerous privacy and security concerns as it moves forward on legislation related to the Internet of Things.

Telemarketing Protections for Consumers Must Be Strengthened

The Telephone Consumer Protection Act ("TCPA") is one of the most important and most popular privacy laws in the United States. Nonetheless, we recognize that significant changes in technology and business practices over the past 25 years require the TCPA be updated for the 21st century. We urge this Committee and the Congress to accomplish this goal in a way that continues to protect consumer privacy and takes advantage of available technological solutions. The Spoofing Prevention Act would help further the goal of combatting unwanted telemarketing messages by modernizing and strengthening the tools available to the public.

Road for Hackers (2016), https://www.fireeye.com/content/dam/fireeye-www/services/pdfs/connected-cars-the-open-road-for-hackers.pdf.

[10] *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

[11] *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/.

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

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

EPIC has previously advised Congress on an updated approach to combat unwanted telemarketing.[14] This approach should include a requirement that any automated calls reveal (1) the actual identity of the caller and (2) the purpose of the call. Digital networks now make it easier for commercial firms to make known the source and purpose of the call, and this information can then help consumers determine how best to prioritize incoming messages. We urge this Committee to consider additional policy approaches that take advantage of technological developments in ways beneficial to consumer privacy.

We appreciate your consideration of EPIC's perspective and supporting materials on these important issues. EPIC looks forward to working with the Committee on Commerce, Science, and Transportation on these and other issues impacting the privacy and security of American consumers.

Sincerely,

Marc Rotenberg
Marc Rotenberg
EPIC President

Claire Gartland
Claire Gartland
Director, EPIC Consumer Privacy Project

James Graves
James Graves
EPIC Law and Technology Fellow

[14] Letter from EPIC to the U.S. House of Representatives Committee on Energy and Commerce Subcommittee on Communications and Technology, *Modernizing the Telephone Consumer Protection Act* (Sept. 21, 2016), https://epic.org/privacy/telemarketing/EPIC-Modernizing-TCPA.pdf.