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

January 17, 2018

Representative Bob Latta, Chairman
Representative Jan Schakowsky, Ranking Member
House Energy & Commerce Committee
Subcommittee on Digital Commerce & Consumer Protection
2125 Rayburn House Office Building
Washington, D.C. 20515

RE: "Disrupter Series: The Internet of Things, Manufacturing and Innovation"

Dear Chairman Latta and Ranking Member Schakowsky:

We write to you regarding the "Disrupter Series: The Internet of Things, Manufacturing and Innovation" hearing.[1] American consumers face unprecedented privacy and security threats. The unregulated collection of personal data and the growth of the Internet of Things ("IoT") 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' personal data.

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 leader in the field of the Internet of Things and consumer protection.[3] EPIC urged the Federal Trade Commission ("FTC") to establish strong standards to safeguard American consumers.[4] And EPIC has testified before the House Oversight and Government Reform on the risks of "The Internet of Cars."[5]

Privacy, Security, and Physical Safety Risks of the IoT

Many IoT devices feature "always on" tracking technology that surreptitiously records consumers' private conversations in their homes.[6] These "always on" devices raise numerous

[1] *Disrupter Series: The Internet of Things, Manufacturing and Innovation*, 115th Cong. (2018), H. Comm. on Energy and Commerce, Subcomm. On Digital Commerce and Consumer Protection (Jan. 18, 2018), https://energycommerce.house.gov/hearings/disrupter-series-internet-things-manufacturing-innovation/.
[2] *See* EPIC, *About EPIC*, https://epic.org/epic/about.html.
[3] EPIC, "Internet of Things (IoT)," https://epic.org/privacy/internet/iot/
[4] *See* Comments of the Electronic Privacy Information Center ("EPIC") to the FTC on The Privacy and Security Implications of the Internet of Things," (June 1, 2013), https://epic.org/privacy/ftc/EPIC-FTC-IoT-Cmts.pdf; *see also* In re Google Buzz, https://epic.org/privacy/ftc/googlebuzz/; FTC Facebook Settlement, https://epic.org/privacy/ftc/facebook/.
[5] Khaliah Barnes, EPIC Associate Director, *The Internet of Cars,* Testimony, 114th Cong. (2015), H. Comm. on Oversight and Government Reform, Subcomm. on Information Technology and Subcomm. on Transportation and Public Assets, (Nov. 18, 2015), https://epic.org/privacy/edrs/EPIC-Connected-Cars-Testimony-Nov-18-2015.pdf.
[6] 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.

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.[7] Furthermore, software and hardware vulnerabilities also harm consumers. Last year EPIC joined other consumer advocacy groups in a letter to the Consumer Product Safety Commission to urge the agency to recall Google Home Mini.[8] Due to a hardware flaw, the device was always listening to conversations and users could not disable it. Therefore, both the intentional designs and unintentional flaws of IoT devices present risks to consumers.

In addition to privacy risks, the IoT also poses risks to physical security 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]

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.[10] 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.[11] They were also behind the attack on security blogger Brian Krebs' web site, one of the largest attacks ever seen.[12]

Effective Regulation of the IoT

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

---

[7] 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.
[8] Coalition Letter to U.S. Consumer Product Safety Comm. On Google Home Mini (Oct. 13, 2017), https://epic.org/privacy/consumer/Letter-to-CPSC-re-Google-Mini-Oct-2017.pdf.
[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 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/.

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] Moreover, consumers rarely have adequate knowledge about the security of an IoT product when they are determining whether to purchase it. This information asymmetry makes it impossible for market forces to regulate the IoT effectively.

The regulatory environment is currently too weak to protect American consumers. The memo written by majority staff for this hearing points to the FTC as the key regulator of IoT,[14] but the FTC's authority is insufficient to protect consumers. Unlike other federal agencies, the FTC has virtually no rulemaking authority; its ability to regulate is based on ex post facto enforcement actions. This means that the FTC cannot act until after consumers have already been harmed. Other agencies, such as the Consumer Product Safety Commission, should regulate the IoT.[15] Manufacturers could be liable under tort law using products liability theory, but this legal strategy has not been employed much in the courts.[16]

Congress should act to empower regulators to protect consumers from the risks posed by the IoT.

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/ *Christine Bannan*
Christine Bannan
EPIC Policy Fellow

[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).
[14] Committee Majority Staff, Memo to Members of Subcomm. on Digital Commerce and Consumer Protection (Jan. 16, 2018), http://docs.house.gov/meetings/IF/IF17/20180118/106781/HHRG-115-IF17-20180118-SD002.pdf.
[15] *See, e.g.,* EPIC, "Consumer Groups Ask Safety Commission to Recall Google Home," (Oct. 13, 2017), https://epic.org/privacy/internet/iot/
[16] Alan Butler, Products Liability and the Internet of (Insecure) Things: Should Manufacturers Be Liable for Damage Caused by Hacked Devices?, 50 U. Mich. J. L. Reform 913 (2017), http://repository.law.umich.edu/mjlr/vol50/iss4/3.