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

June 19, 2019

The Honorable Jerry Moran, Chairman
The Honorable Richard Blumenthal, Ranking Member
U.S. Senate Committee on Commerce, Science, and Transportation
Subcommittee on Manufacturing, Trade, and Consumer Protection
512 Dirksen Senate Office Building
Washington, DC 20510

Dear Chairman Moran and Ranking Member Blumenthal:

We write to you regarding the oversight hearing for the Consumer Product Safety Commission.[1] We write to call your attention to the ongoing failure of the CPSC to address the growing risk to privacy and security of Internet-connected devices. The unregulated collection of personal data and the growth of the Internet of Things ("IoT")[2] has led to staggering increases in identity theft, security breaches, and new cybersecurity threats. The CPSC should regulate Internet-connected devices. Privacy and security are integral to consumer safety.

EPIC is a public interest research center established in 1994 to focus public attention on emerging privacy and civil liberties issues.[3] EPIC is a leading advocate for consumer privacy, and has led the effort to establish the authority of the Federal Trade Commission ("FTC") to safeguard consumer privacy and more recently to explore the impact of the Internet of Things.[4] EPIC also urged the Consumer Product Safety Commission ("CPSC") to address the hazards of weak privacy and security in IoT products.[5]

Today, the IoT network is the weak link in consumer products. IoT devices track personal data generated by consumers' activities and lifestyles. IoT devices pose significant privacy concerns that could threaten physical danger.

EPIC brought the Google Home Mini complaint[6] to the CPSC precisely because the design defect of the consumer device created a specific risk to consumers. The Acting Chairman of the

[1] *Oversight of the Consumer Product Safety Commission*, 116th Cong. (2019), S. Comm. on Commerce, Sci. & Trans., Subcomm. on Manufacturing, Trade, and Consumer Protection, https://www.commerce.senate.gov/public/index.cfm/2019/6/oversight-of-the-consumer-product-safety-commission (Jun. 20, 2019).
[2] EPIC, Internet of Things (IoT), https://epic.org/privacy/internet/iot/.
[3] *See* EPIC, *About EPIC*, https://epic.org/epic/about.html.
[4] EPIC Comments to the Federal Trade Comm'n, *On the Privacy and Security Implications of the Internet of Things* (June 1, 2013), https://epic.org/privacy/ftc/EPIC-FTC-IoT-Cmts.pdf.
[5] Sunny Kang, EPIC International Consumer Counsel, *The Internet of Things and Consumer Product Hazards*, Testimony, CPSC (May 16, 2018), https://www.youtube.com/watch?v=-YSDEkWuxUo&feature=youtu.be.
[6] 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.

CPSC responded to EPIC, stating that "CPSC's authority will not generally extend to situations solely related to consumer privacy or data security, that do not pose a risk of physical injury or illness, or property damage."[7]

The CPSC response reflects a profound lack of understanding about the IoT and the new threats facing consumers. As renowned security expert Bruce Schneier has said: "The Internet is dangerous—and the IoT gives it not just eyes and ears, but also hands and feet. Security vulnerabilities, exploits, and attacks that once affected only bits and bytes now affect flesh and blood."[8]

Hackers, criminals, and foreign adversaries exploit IoT vulnerabilities to launch network attacks that cause millions of dollars in damage and have devastating impacts on real people.[9] Hackers could conceivably exploit vulnerabilities on "smart" refrigerator to carry out a denial of service attack against the network of a city or hospital. In the past few months alone there have been several such attacks. A ransomware attack known as SamSam took down the entire municipality of Farmington, New Mexico and two hospitals by exploiting vulnerabilities in IoT devices.[10] The city of Atlanta spent 2.6 million dollars to recover from a ransomware attack that impacted municipal functions including the Police Department and the judicial system.[11] It would defy reason to say that unsecured IoT devices do not harm consumers.

Privacy and security hazards should be regulated in the manufacture and design of consumer products. Companies have little incentive to maintain strong standards without regulation. And consumers do not have enough information to evaluate the privacy and security of these products themselves. This has alarming implications for toys that target children's data, and internet-connected home systems like smoke detectors and security cameras.

Therefore, manufacturers—not consumers—must bear the responsibility to ensure the security of their products.[12] We agree with the UK Government's assessment that "There is a need to move away from placing the burden on consumers to securely configure their devices, and instead ensure that strong security is built in by design."[13]

---

[7] CPSC Acting Chairman Ann Marie Buerkle, *Response to EPIC and Consumer Privacy Organizations* (March 23, 2018), https://epic.org/CPSC-response-GoogleHomeMini-3.23.18.pdf.
[8] Bruce Schneier, *IoT Cybersecurity: What's Plan B?*, Schneier on Security (Oct. 18, 2017), https://www.schneier.com/blog/archives/2017/10/iot_cybersecuri.html.
[9] Bruce Schneier, *Click Here to Kill Everyone*, N.Y. Magazine (Jan. 27, 2017), http://nymag.com/selectall/2017/01/the-internet-of-things-dangerous-future-bruce-schneier.html (describing an attack that used millions of DVRs and other insecure IoT devices to take down Twitter, Netflix, Reddit, and other sites down from the internet).
[10] Bill Siwicki, *71% of IoT medical device ransomware infections caused by user practice issues*, Healthcare IT News (March 5, 2018), http://www.healthcareitnews.com/news/71-iot-medical-device-ransomware-infections-caused-user-practice-issues.
[11] Lily Hay Newman, *Atlanta Spent $2.6M to Recover from a $52,000 Ransomware Scare*, Wired (April 23, 2018), https://www.wired.com/story/atlanta-spent-26m-recover-from-ransomware-scare/.
[12] *See* 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/cgi/viewcontent.cgi?article=1193&context=mjlr.
[13] UK Department for Digital, Culture, Media & Sport, *Secure by Design: Improving the cyber security of consumer Internet of Things Report* (March 2018),

Current voluntary standards are lax. And current safety regulations are outdated. They are not adequate to address the security hazards of IoT devices. The CPSC should establish mandatory privacy and security standards, and require certification to these standards before IoT devices are allowed into the market stream.

The code of practice proposed by the UK government serves as a useful framework for security standards for IoT. In particular, manufacturers should adopt the following:[14]

1. No default passwords
2. Implement a vulnerability disclosure policy
3. Keep software updated
4. Securely store credentials and security-sensitive data
5. Communicate securely
6. Minimize exposed attack surfaces
7. Ensure software integrity
8. Data protection
9. Make systems resilient to outages
10. Monitor system telemetry data
11. Make it easy for consumers to delete personal data
12. Make installation and maintenance of devices easy
13. And validate input data

This guidance necessitates privacy and security by design. If the CPSC implements this code of practice, it will shift the responsibility of product safety back to manufacturers where it belongs.

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,

Marc Rotenberg
Marc Rotenberg
EPIC President

Caitriona Fitzgerald
Caitriona Fitzgerald
EPIC Policy Director

Enclosure:
EPIC and Consumer Privacy Organizations Letter to CPSC, *Recall Google Home Mini* (Oct. 13, 2017)

https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/686089/Secure_by_Design_Report_.pdf.
[14] *Id.*