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

"The Internet of Things and Consumer Products Hazards"

Consumer Product Safety Commission

May 16, 2018 Hearing

Oral Presentation

Privacy and security are integral to consumer safety. And today the "Internet of Things" (IoT) is the weak link in all privacy and security related matters for the consumer products. The "Consumer Product Safety Commission" has a responsibility to protect consumers from the risks these devices create. Holding a hearing in the year 2018 to discuss the consumer safety issues of IoT without addressing privacy and security concerns is akin to holding a hearing in the last century about kitchen appliances without addressing the risk that a toaster or small grill might catch fire because of inadequate wiring.

The Electronic Privacy Information Center ("EPIC") is a public interest research established in 1994 to focus public attention on emerging privacy and civil liberties issues.[1] Last fall, EPIC and a coalition of consumer groups wrote to the CPSC urging the Commission to recall the Google Home Mini because the device had a manufacturing defect that allowed Google to intercept and record private conversations in homes without the knowledge or consent of the consumer.[2] We brought the complaint to the CPSC and not the FTC precisely because the defect in the design of the device, intended for the consumer marketplace, created a specific privacy and security risk to consumers who purchased the product.

[1] EPIC, *About EPIC*, https://epic.org/epic/about.html.
[2] EPIC and Consumer Privacy Organizations Letter to CPSC, *Recall Google Home Mini* (Oct. 13, 2017), https://epic.org/privacy/consumer/Letter-to-CPSC-re-Google-Mini-Oct-2017.pdf.

We received a response from the Acting Chairman of the CPSC, 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 that could result in injury or illness."[3]

The assessment reflects a lack of understanding about the Internet of Things and the new threats facing consumers. As renowned security expert and EPIC advisory board member 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."[4] If the CPSC ignores the dangers posed by IoT it will be ignoring its Congressional mandate to protect consumers.

The consumer hazards created by IoT devices extend far beyond "fire, burn, shock, tripping or falling, laceration, contusion, and chemical exposure" contemplated by the Federal Register notice for this hearing.[5] Poorly secured IoT devices are used for botnets that launch denial of service or other network attacks that can cause millions of dollars in property damage and have devastating impacts on consumers.[6] Hackers could conceivably exploit vulnerabilities on your "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

[3] 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.
[4] 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.
[5] CPSC, *The Internet of Things and Consumer Product Hazards*, Fed. Reg. (March 27, 2018), https://www.federalregister.gov/documents/2018/03/27/2018-06067/the-internet-of-things-and-consumer-product-hazards.
[6] 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).

hospitals by exploiting vulnerabilities in IoT devices.[7] The city of Atlanta spent $2.6 million to recover from a ransomware attack that impacted municipal functions including the Police Department and the judicial system.[8] It would defy reason to say that these consequences of insecure IoT devices do not harm consumers.

The same rationales for regulating the manufacturing and design hazards of consumer products apply to regulating privacy and security hazards. Consumers do not have enough information to evaluate products based on safety or security and companies have little incentive to maintain strong standards without regulation. Manufacturers—not consumers—must bear the responsibility to ensure the products that they offer for sale are safe for use by consumers.[9] 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."[10]

Current voluntary standards and safety regulations do not adequately address the hazards specific to IoT devices. The CPSC should establish mandatory security standards for IoT devices and certification to its standards be required before IoT devices are allowed in the marketplace. The code of practice proposed by the UK government provides thirteen rules that serve as a useful framework for manufacturers of consumer IoT products:[11]

---

[7] 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.
[8] 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/.
[9] *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.
[10] UK Department for Digital, Culture, Media & Sport, *Secure by Design: Improving the cyber security of consumer Internet of Things Report* (March 2018), https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/686089/Secure_by_Design_Report_.pdf.
[11] *Id.*

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. Ensure that personal data is protected
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. Validate input data

If the CPSC implements this code of practice, it will shift the responsibility of product safety and security back to manufacturers where it belongs.

We thank the Commission for the opportunity to testify and look forward to working together on this critical consumer safety issue.

Sincerely,

/s/ *Marc Rotenberg*
Marc Rotenberg
EPIC President

/s/ *Christine Bannan*
Christine Bannan
EPIC Administrative Law and Policy Fellow