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

May 21, 2018

The Honorable Bob Latta
The Honorable Jan Schakowsky
House Committee on Energy and Commerce
Subcommittee on Digital Commerce and Consumer Protection
2322 Rayburn House Office Building
Washington, D.C. 20515

Dear Chairman Latta and Ranking Member Schakowsky:

We write to you regarding the upcoming hearing on "Internet of Things Legislation."[1] American consumers face unprecedented privacy and security threats. 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 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.[3] EPIC is a leading advocate for consumer privacy, and has actively participated in the proceedings of the Federal Trade Commission ("FTC") including 2013 comments on the Internet of Things.[4] And in 2015, EPIC testified at a hearing on "The Internet of Cars" before the House Oversight and Government Reform.[5] EPIC recently submitted comments[6] to the Consumer Product Safety Commission ("CPSC") on the hazards caused by weak privacy and security in IoT products and testified before the Commission.[7]

Privacy, Security, and Physical Safety Risks of the IoT

[1] *Internet of Things Legislation*, 115th Cong. (2018), H. Comm. on Energy and Commerce, Subcomm. on Digital Commerce and Consumer Protection (May 22, 2018), https://energycommerce.house.gov/hearings/internet-of-things-legislation/.
[2] EPIC, Internet of Things (IoT), https://epic.org/privacy/internet/iot/.
[3] *See* EPIC, *About EPIC*, https://epic.org/epic/about.html.
[4] https://epic.org/privacy/ftc/EPIC-FTC-IoT-Cmts.pdf
[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 Comments to CPSC, *The Internet of Things and Consumer Product Hazards* (May 2, 2018), https://epic.org/apa/comments/EPIC_CPSC_IoT_May2018.pdf.
[7] 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.

Many IoT devices feature "always on" tracking technology that surreptitiously records consumers' private conversations in their homes.[8] 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.[9]

Furthermore, software and hardware vulnerabilities also harm consumers. Last year EPIC joined other consumer advocacy groups in a letter to the CPSC to urge the agency to recall Google Home Mini.[10] Due to a hardware flaw, the device was always listening to conversations and users could not disable it. Therefore, both the intentional designs (e.g., Amazon Alexa) and unintentional flaws (e.g., Google Home Mini) 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.[11]

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.[12] 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.[13] They were also behind the attack on security blogger Brian Krebs' web site, one of the largest attacks ever seen.[14]

---

[8] 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.
[9] 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.
[10] 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.
[11] *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.
[12] *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
[13] *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/.
[14] *See* Brian Krebs, *KrebsOnSecurity Hit With Record DDoS*, KrebsOnSecurity (Sept. 21, 2016), https://krebsonsecurity.com/2016/09/krebsonsecurity-hit-with-record-ddos/.

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 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.[15] 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 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. Manufacturers could be liable under tort law using products liability theory, but this legal strategy has not been employed much in the courts.[16]

Consumer Product Safety Commission

It is incumbent upon the CPSC to regulate the privacy and security of IoT devices. Privacy and security are integral to consumer safety. And today, the Internet of Things are the weakest link to privacy and security vulnerabilities in consumer products. IoT devices track personal data by seamlessly integrating into the consumers' activities and lifestyles. They blend into everyday objects. Thus, the ubiquity of IoT sensors and their amassment of granular data pose significant privacy concerns that could threaten physical danger.

We brought the Google Home Mini complaint[17] to the CPSC and not the FTC, precisely because the design defect of the device, intended for the consumer marketplace, created a specific privacy and security risk to consumers. 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."[18]

This assessment reflects a lack of understanding about the Internet of Things and the new threats facing consumers. As renowned security expert Bruce Schneier has said: "The Internet is

---

[15] Testimony of Bruce Schneier before the House Committee on Energy & Commerce, *Understanding the Role of Connected Devices in Recent Cyber Attacks*, 114th Cong. (2016).
[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.
[17] *See supra* note 7.
[18] 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.

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."[19]

Poorly secured IoT devices are used for botnets that launch network attacks that can cause millions of dollars in property damage and have devastating impacts on real people.[20] 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 hospitals by exploiting vulnerabilities in IoT devices.[21] 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.[22] It would defy reason to say that unsecured IoT devices do not harm consumers.

Privacy and security hazards should be regulated in the manufacturing 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.[23] 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."[24]

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.

---

[19] 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.

[20] 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).

[21] 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.

[22] 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/.

[23] *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.

[24] 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.

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:[25]

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,

/s/ *Marc Rotenberg*
Marc Rotenberg
EPIC President

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

[25] *Id.*