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

March 5, 2018

The Honorable Marsha Blackburn, Chair
The Honorable Michael Doyle, Ranking Member
U.S. House Committee on Energy and Commerce
Subcommittee on Communications and Technology
2125 Rayburn House Office Building
Washington, D.C. 20515

RE: Oversight of the National Telecommunications and Information Administration

Dear Chairwoman Blackburn and Ranking Member Doyle:

We write to you regarding tomorrow's hearing on "Oversight of the National Telecommunications and Information Administration."[1] American consumers face unprecedented privacy and security threats. The unregulated collection of personal data has led to staggering increases in identity theft, security breaches, and financial fraud in the United States.[2] Congress should work with the NTIA to develop meaningful safeguards for the privacy and security of Americans' personal information.

The Electronic Privacy Information Center was established in 1994 to focus public attention on emerging privacy and civil liberties issues. EPIC is a leading advocate for consumer privacy and has appeared before this Committee on several occasions, and has actively participated in the proceedings of the Federal Trade Commission ("FTC") and the Federal Communications Commission ("FCC").[3]

---

[1] *Oversight of the National Telecommunications and Information Administration*, 115th Cong. (2018), H. Comm. on Energy & Commerce, Subcomm. on Communications and Technology, https://energycommerce.house.gov/hearings/oversight-national-telecommunications-information-administration/ (Mar. 6, 2018).

[2] Federal Trade Comm'n, *Privacy & Data Security Update: 2017*, *available at* https://www.ftc.gov/system/files/documents/reports/privacy-data-security-update-2017-overview-commissions-enforcement-policy-initiatives-consumer/privacy_and_data_security_update_2017.pdf

[3] *See, e.g,* Marc Rotenberg, EPIC Executive Director, Testimony before the U.S. House Energy & Commerce Subcommittee on Communications and Technology, *Examining the EU Safe Harbor Decision and Impacts for Transatlantic Data Flows* (November 13, 2015), https://epic.org/privacy/intl/schrems/EPIC-EU-SH-Testimony-HCEC-11-3-final.pdf; Marc Rotenberg, EPIC Executive Director, Testimony before the U.S. House Energy & Commerce Subcommittee on Communications and Technology, *Communications Networks and Consumer Privacy: Recent Developments* (April 23, 2009), https://epic.org/privacy/dpi/rotenberg_HouseCom_4-09.pdf; Letter from EPIC to the U.S. House Committee on Energy and Commerce on FCC Privacy Rules (June 13, 2016), https://epic.org/privacy/consumer/EPIC-FCC-Privacy-Rules.pdf; Letter from EPIC to the U.S. Senate Committee on Commerce, Science, and Transportation on FTC Oversight (Sept. 26, 2016), https://epic.org/privacy/consumer/EPIC-Letter-Sen-Comm-CST-FTC-Oversight.pdf.

The recent Equifax data breach that exposed the personal information of more than 145 million Americans is the latest in a growing number of high-profile hacks that threaten the privacy, security, and financial stability of American consumers. Far too many organizations collect, use, and disclose detailed personal information with too little regard for the consequences. Further, there are massive privacy and security implications of the growing "Internet of Things." Many IoT devices feature "always on" tracking technology that surreptitiously records consumers' private conversations in their homes.[4] Companies say that the devices rely on key words, but to detect those words, the devices must always be listening. Congress and the NTIA must work together to enact concrete consumer protections that:

- Promote Privacy Enhancing Techniques (PETs) that minimize or eliminate the collection of personal information.[5]
- Ensure routine security updates for IoT devices; and
- Carefully assesses IoT deployment for critical functions, including transportation, home security, and medical devices.

The NTIA's multi-stakeholder processes for addressing these challenges simply do not work – they result in weak, voluntary self-regulatory regimes. Industry self-regulatory programs do not provide meaningful privacy protections.[6] The NTIA should support a strong legal framework that protects American Internet users and promotes public safety.

The implications of Internet of Things for consumer privacy and security are far-reaching. If the NTIA fails to develop appropriate safeguards, the country will face growing risk.

We ask that this letter be entered in the hearing record. EPIC looks forward to working with the Subcommittee on Communications and Technology on these issues.

Sincerely,

Marc Rotenberg
Marc Rotenberg
EPIC President

Caitriona Fitzgerald
Caitriona Fitzgerald
EPIC Policy Director

Christine Bannan
Christine Bannan
EPIC Administrative Law and Policy Fellow

---

[4] 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.
[5] *See* Comments of EPIC, *On the Privacy and Security Implications of the Internet of Things*, FTC File No. ___ (June 1, 2013), https://epic.org/privacy/ftc/EPIC-FTC-IoT-Cmts.pdf.
[6] Comments of EPIC, *Multistakeholder Process to Develop Consumer Data Privacy Codes of Conduct*, Docket No. 120214135-2135-01 (Apr. 2, 2012), https://epic.org/privacy/consumer/EPIC-NTIA-Comments-FINAL.pdf; Comments of EPIC, *Protecting the Privacy of Customers of Broadband and Other Telecommunications Services*, WC Docket NO. 16- 106 (July 6, 2016), https://epic.org/apa/comments/EPIC-FCC-Privacy-NPRM-Reply-Comments-07.06.16.pdf.