November 15, 2017

The Honorable John Ratcliffe, Chairman
The Honorable Cedric L. Richmond, Ranking Member
U.S. House Committee on Homeland Security
Subcommittee on Cybersecurity and Infrastructure Protection
H2-176 Ford House Office Building
Washington, DC 20515

Dear Chairman Ratcliffe and Ranking Member Richmond:

We write to you regarding the hearing on “Maximizing the Value of Cyber Threat Information Sharing.” EPIC is a public interest research center established in 1994 to focus public attention on emerging privacy and civil liberties issues. We are particularly interested in the privacy issues raised by the government’s cybersecurity policies that implicate the collection and use of personal data.

At the end of 2015, the Cybersecurity Act of 2015 was signed into law. Title of I of that act, known as the Cybersecurity Information Sharing Act of 2015 (CISA), created a mechanism for the federal government to disseminate cyber threat information to the private sector and for the private sector to provide cyber threat information to the federal government. Much of that information concerns the activities of individual Internet users.

CISA and earlier bills, such as the Cyber Intelligence Sharing and Protection Act (CISPA), were criticized for the potential to compromise American’s privacy. With passage of

---

2 See About EPIC, EPIC.org, https://epic.org/epic/about.html.
4 Id.
the Cybersecurity Act of 2015, the risk to privacy still remains.\(^6\) The bill relies on a complex procedure to “scrub” identifying information from the computer logs that are turned over by private firms to the federal government. This information is explicitly acquired without the privacy safeguards that would otherwise apply under the federal wiretap.

Effective oversight of the government’s collection and use of personal data is particularly important in the realm of cybersecurity where it is easy to obtain vast troves of personal information with little accountability. The history of the U.S. government’s surveillance of domestic communications in collaboration with private companies\(^7\) makes it imperative that Congress ensure that CISA safeguards Americans’ privacy.

We urge you to ask detailed questions about the dissemination of information from companies to the government, including:

1. What personal information is disseminated to the government in the context of providing cyber threat information?
2. What processes do you use to mitigate the privacy risks before providing cyber threat information to the government?
3. What are the privacy risks with the current mechanism to provide cyber threat information to the government?
4. What more could be done to safeguard the personal data of Americans?

We ask that this letter be entered in the hearing record. EPIC looks forward to working with the Subcommittee on these issues of vital importance to the American public.

Sincerely,

/s/ Marc Rotenberg  /s/ Caitriona Fitzgerald
Marc Rotenberg  Caitriona Fitzgerald
EPIC President  EPIC Policy Director

/s/ Jeramie Scott
Jeramie Scott
EPIC National Security Counsel

---
