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

April 23, 2017

The Honorable Ron Johnson, Chairman
The Honorable Claire McCaskill, Ranking Member
U.S. Senate Committee on Homeland Security & Government Affairs
340 Dirksen Senate Office Building
Washington, DC 20510

RE: Hearing on Cyber Threats Facing America: An Overview of the Cybersecurity Threat Landscape

Dear Chairman Johnson and Ranking Member McCaskill:

We write to you regarding the "Mitigating America's Cybersecurity Risk" hearing.[1] EPIC has an active interest in this effort. Weaknesses in cyber security threaten both consumers and democratic institutions.[2] We welcome your leadership on this critical issue and look forward to opportunities to work with you and your staff.

EPIC is a public interest research center established in 1994 to focus public attention on emerging privacy and civil liberties issues.[3] EPIC is also a leading advocate for civil liberties and democratic values in the information age. In response to the finding of the Intelligence Community that the Russian government interfered with the 2016 Presidential election, EPIC launched a new project on Democracy and Cybersecurity.[4] Our goal is to determine the extent of Russian interference and ensure that the U.S. government takes necessary steps to safeguard political institutions against future attack.

Data protection and privacy should remain a central focus of the cyber security policy of the United States. It is precisely the extensive collection of personal information without adequate safeguards that places the United States at risk from cyber criminals and foreign adversaries. In 2015, more than 22 million records of federal employees, including 5 million digitized fingerprints and the sensitive form SF-86, were compromised. So-called "credit monitoring services" are an insufficient response to the ongoing risk to the financial records, medical records, and private communications of Americans.

---

[1] *Mitigating America's Cybersecurity Risk*, 115th Cong. (2018), S. Comm. on Homeland Security and Gov't Affairs, https://www.hsgac.senate.gov/hearings/mitigating-americas-cybersecurity-risk (Apr. 24, 2018).
[2] *See* Democracy and Cybersecurity: Preserving Democratic Institutions, EPIC, https://epic.org/democracy/.
[3] *See* EPIC, *About EPIC*, https://epic.org/epic/about.html.
[4] *See* EPIC, *Democracy and Cybersecurity*, https://epic.org/democracy/.

Strong encryption policy and robust technical measures must be enacted to safeguard personal data. Weaknesses in security standards create vulnerabilities for American businesses and consumers that will be exploited by foreign adversaries. Where it is possible to minimize or eliminate the collection of personally identifiable information, the risk to the American public will be reduced. Strong encryption keeps the information of the American people secure, which by extension makes the nation secure. And perhaps it is a firewall and not a border wall that the United States needs to safeguard its national interests at this moment in time.[5]

The Cyber Security Information "Sharing" Act is now in force. That law facilitates the transfer of customer and client data from the private sector to the government, raising widespread concerns among technical experts and privacy organizations about the protection of personal information. While we favor a cooperative relationship between companies and the federal government concerning cyber security, the federal government must respect the privacy obligations of private companies and ensure the transparency of its own conduct. In the cyber security domain, as with other programs supported by taxpayer dollars, the government must uphold the law and remain open and accountable.

Finally, *Congress should strengthen the federal Privacy Act*. Personal data stored in federal agencies remains one of the key targets of criminal hackers and foreign adversaries. Significant steps were taken by the last administration to establish a Federal Privacy Council and to coordinate privacy protection across the federal agencies. Still, more should be done, including updates to the federal privacy law and the establishment of a data protection agency in the United States.

The United States should stand for the protection of democratic institutions, the rule of law, an independent judiciary and the protection of fundamental rights. Our national security strategy should reflect these values.

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

Sincerely,

/s/ *Marc Rotenberg*
Marc Rotenberg
EPIC President

/s/ *Caitriona Fitzgerald*
Caitriona Fitzgerald
EPIC Policy Director

/s/ *Christine Bannan*
Christine Bannan
EPIC Policy Fellow

[5] Garry Kasparov (@kasparov63), "If the US is serious about stopping a real danger from abroad, it should build a better firewall, not a bigger border wall." (12:34 PM - 22 Jan 2018), https://twitter.com/Kasparov63/status/955539139121819649.