epic.org

Electronic Privacy Information Center
1519 New Hampshire Avenue NW
Washington, DC 20036, USA

+1 202 483 1140
+1 202 483 1248
@EPICPrivacy
https://epic.org

December 9, 2019

The Honorable Lindsey Graham, Chairman
The Honorable Dianne Feinstein, Ranking Member
U.S. Senate Committee on the Judiciary
Dirksen Senate Office Building 224
Washington, DC 20510

Dear Chairman Graham and Ranking Member Feinstein:

We write to you regarding the "Encryption and Lawful Access: Evaluating Benefits and Risks to Public Safety and Privacy" hearing.[1] EPIC has an active interest in this effort. America is facing an epidemic of data breach and identify theft. Now is not the time to undermine the systems that we all rely upon to secure our data and communications.

EPIC is a public interest research center established in 1994 to focus public attention on emerging privacy and civil liberties issues.[2] EPIC has advocated for strong encryption since its founding[3], and consistently pushed back against efforts to weaken the technology.[4] EPIC has also played a key role in the development of the international framework for cryptography policy that favored the deployment of strong security measures to safeguard personal information. EPIC published the first comparative studies of international encryption policy.[5]

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. Strong encryption keeps the information of the American people secure, which by extension makes the nation secure. Leading computer scientists and security experts have found that proposals to add "backdoors" for law enforcement are

---

[1] *Encryption and Lawful Access: Evaluating Benefits and Risks to Public Safety and Privacy*, S. Comm. on the Judiciary (Dec. 9, 2019), https://www.judiciary.senate.gov/meetings/encryption-and-lawful-access-evaluating-benefits-and-risks-to-public-safety-and-privacy.
[2] *See* EPIC, *About EPIC*, https://epic.org/epic/about.html.
[3] See e.g., EPIC, *The Clipper Chip*, https://epic.org/crypto/clipper/.
[4] *See e.g., On Internet Privacy and Profiling Before S. Comm. on Commerce*, 106th Cong. (2000) (statement of Marc Rotenberg, Executive Director, EPIC), https://epic.org/privacy/internet/senate-testimony.html; *The Security and Freedom Through Encryption Act (SAFE) H.R. 695 Before the Subcomm. on Courts and Intellectual Property of the H. Comm. on the Judiciary*, 105th Cong. (1997) (statement of Marc Rotenberg, Executive Director, EPIC), https://epic.org/crypto/export_controls/epic_safe_testimony_397.html; Letter from EPIC to David Kaye, U.N. Special rapporteur, Office of the High Comm'r for Human Rights (Feb. 10, 2015), https://epic.org/misc/EPIC-UNCHR-ltr-02-2015.pdf; EPIC, *EPIC v. FBI*, https://epic.org/amicus/crypto/apple/.
[5] EPIC, *Cryptography and Liberty 1998: An International Survey of Encryption Policy* (1998).

"unworkable in practice, raise enormous legal and ethical questions, and would undo progress on security at a time when Internet vulnerabilities are causing extreme economic harm."[6]

Protecting electronic devices such as cell phones and Internet of Things devices from criminals and others who seek to exploit valuable personal data requires more than just legal protection. Data protection requires robust encryption and other security techniques to prevent third parties from gaining access to the contents of a person's electronic devices. Consumers demand such protections, and Apple and other companies have responded by creating strong digital locks that are designed to keep all others, even the company, from accessing the contents of user devices. Like traditional locks, these devices protect consumers from crime and reduce the risk of theft. And, like traditional locks, they are always subject to attack by determined criminals. No company should be compelled to weaken their digital locks because, if they do, consumers will suffer, crime will increase, and any short-term benefit that law enforcement may obtain will be more than outweighed by the increase in crime across the country that will result.

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.[7]

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/ *Alan Butler*
Alan Butler
EPIC Senior Counsel

[6] Ross Anderson, Whitfield Diffie, Peter G. Neumann, Ronald Rivest, Bruce Schneier, et al., *Keys Under Doormats: Mandating Insecurity by Requiring Gov't Access to All Data and Communications* (July 2015), https://www.schneier.com/academic/paperfiles/paper-keys-under-doormats-CSAIL.pdf.
[7] EPIC, *The U.S. Urgently Needs a Data Protection Agency*, https://epic.org/dpa/.