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

October 29, 2019

The Honorable Janice D. Schakowsky, Chair
The Honorable Cathy McMorris Rodgers, Ranking Member
U.S. House Committee on Energy and Commerce
Subcommittee on Consumer Protection & Commerce
2125 Rayburn House Office Building
Washington, D.C. 20515

Dear Chairwoman Schakowsky and Ranking Member McMorris Rodgers:

We write to you in regarding your hearing on "Reauthorizing Brand USA and the U.S. SAFE WEB Act."[1] EPIC appreciates the Committee's focus on cross-border fraud. Fraudulent and deceptive business practices that would otherwise be prosecuted in the United States should not be beyond the reach of U.S. law enforcement simply because an operator sets up shop outside the country. In similar fashion, government agencies seeking to protect the interests of consumers in their jurisdictions should expect the cooperation of the Federal Trade Commission when cross-border problems emerge.

EPIC has a particular interest in the protection of consumers in the global economy. EPIC testified before this Committee and the Senate Commerce Committee on the Safe WEB Act (then the "International Consumer Protection Enforcement Act") in 2003.[2] EPIC also works closely with consumer and civil liberties organizations, such as the Trans Atlantic Consumer Dialogue (TACD), and the OECD on the development of international policy to protect consumers.

The Safe WEB Act should be reauthorized – cross-border enforcement and cooperation is critical for effective protection of US consumers. But it is just as critical for effective protection that Congress enact a comprehensive baseline privacy legislation and establish a U.S Data Protection Agency.

[1] *Reauthorizing Brand USA and the U.S. SAFE WEB Act*, H. Comm. on Energy & Commerce, Subcomm. on Consumer Protection & Commerce (Oct. 29, 2019), https://energycommerce.house.gov/committee-activity/hearings/rescheduled-hearing-on-reauthorizing-brand-usa-and-the-us-safe-web-act.
[2] *Hearing on the International Consumer Protection Act of 2003*, H. Comm. on Energy & Commerce, Subcomm. on Commerce, Trade, and Consumer Protection (Sept. 17, 2003) (Testimony of Marc Rotenberg, EPIC Executive Director), https://epic.org/privacy/whois/testimony.html; *Hearing on Consumer Fraud, the International Consumer Protection Enforcement Act of 2003, and FTC Reauthorization*, S. Comm. on Commerce, Sci., and Trans., Subcomm. on Competition, Foreign Commerce, and Infrastructure (June 11, 2003) (Testimony of Marc Rotenberg, EPIC Executive Director), https://epic.org/privacy/internet/ftc/epic_testimony_june_2003.pdf.

EPIC recently released *Grading on a Curve: Privacy Legislation in the 116th Congress.*[3] EPIC's report set out the key elements of a privacy law. As the Committee and Congress also considers comprehensive data privacy legislation, EPIC recommends:

Strong definition of personal data

The scope of a privacy bill is largely determined by the definition of "personal data." A good definition recognizes that personal data includes both data that is explicitly associated with a particular individual and also data from which it is possible to infer the identity of a particular individual. Personal data also includes all information about an individual, including information that may be publicly available, such as zip code, age, gender, and race. All of these data elements are part of the profiles companies create and provide the basis for decision-making about the individual.

Establishment of an Independent Data Protection Agency

Almost every democratic country in the world has an independent federal data protection agency, with the competence, authority, and resources to help ensure the protection of personal data. These agencies act as an ombudsman for the public. The U.S. has tried for many years to create agencies that mimic a privacy agency, such as the Privacy and Civil Liberties Oversight Board, or to place responsibilities at the FTC. Many now believe that the failure to establish a data protection agency in the U.S. has contributed to the growing incidents of data breach and identity theft. There is also reason to believe that the absence of a U.S. data protection agency could lead to the suspension of transborder data flows following recent decisions of the Court of Justice of the European Union.[4]

Individual rights (right to access, control, delete)

Privacy legislation must give individuals meaningful control over their personal information held by others. This is accomplished by the creation of legal rights that individuals exercise against companies that choose to collect and use their personal data. These rights typically include the right to access and correct data, to limit its use, to ensure it is security protected, and also that it is deleted when no longer needed. "Notice and consent" has little to do with privacy protection. This mechanism allows companies to diminish the rights of consumers, and use personal data for purposes to benefit the company but not the individual.

Strong data controller obligations

Organizations that choose to collect and use personal data necessarily take on obligations for the collection and use of the data. These obligations help ensure fairness, accountability, and transparency in decisions about individuals. Together with the rights of individuals describes above, they are often described as "Fair Information Practices." Many of these obligations are found today in U.S. sectoral laws, national laws, and international conventions. These obligations include:

- Transparency about business practices
- Data collection limitations
- Use/Disclosure limitations
- Data minimization and deletion
- Purpose specification
- Accountability
- Data accuracy
- Confidentiality/security

[3] *See* https://epic.org/GradingOnACurve/.
[4] EPIC, Max Schrems v. Data Protection Commissioner (CJEU - "Safe Harbor"), https://epic.org/privacy/intl/schrems/.

Require Algorithmic Transparency

As automated decision-making has become more widespread, there is growing concern about the fairness, accountability, and transparency of algorithms. All individuals should have the right to know the basis of an automated decision that concerns them. Modern day privacy legislation typically includes provisions for the transparency of algorithms to help promote auditing and accountability.

Require Data Minimization and Privacy Innovation

Many U.S. privacy laws have provisions intended to minimize or eliminate the collection of personal data. Data minimization requirements reduce the risks to both consumers and businesses that could result from a data breach or cyber-attack.

Good privacy legislation should also promote privacy innovation, encouraging companies to adopt practices that provide useful services and minimize privacy risk. Privacy Enhancing Techniques ("PETs") seek to minimize the collection and use of personal data.

Prohibit take-it-or-leave-it or pay-for-privacy terms

Individuals should not be forced to trade basic privacy rights to obtain services. Such provisions undermine the purpose of privacy law: to ensure baseline protections for consumers.

Private Right of Action

Privacy laws in the U.S. typically make clear the consequences of violating a privacy law. Statutory damages, sometimes called "liquidated" or "stipulated" damages are a key element of US privacy law and should provide a direct benefit to those whose privacy rights are violated. The FTC is ineffective. The agency ignores most complaints it receives, does not impose fines on companies that violate privacy, and is unwilling to impose meaningful penalties on repeat offenders.[5]

Limit Government Access to Personal Data

Privacy legislation frequently includes specific provisions that limit government access to personal data held by companies. These provisions help ensure that the government collects only the data that is necessary and appropriate for a particular criminal investigation. Without these provisions, the government would be able to collect personal data in bulk from companies, a form of "mass surveillance" enabled by new technologies. The Supreme Court also recently said in the *Carpenter* case that personal data held by private companies, in some circumstances, is entitled to Constitutional protection.[6]

Do Not Preempt Stronger State Laws

A well-established principle in the United States is that federal privacy law should operate as a floor and not a ceiling. The consequences of federal preemption are potentially severe and could include both a reduction in privacy protection for many consumers, particularly in California, and

[5] Dissenting Statement of Commissioner Rohit Chopra, *In re Facebook, Inc.*, FTC File No. 1823109 at 17 (July 24, 2019), https://www.ftc.gov/system/files/documents/public_statements/1536911/chopra_dissenting_statement_on_facebook_7-24-19.pdf.

[6] *Carpenter v. United States*, 138 S. Ct. 2206, 2223 (2018).

also a prohibition on state legislatures addressing new challenges as they emerge. That could leave consumers and businesses exposed to increasing levels of data breach and identity theft from criminal hackers and foreign adversaries.

Even as the Federal Trade Commission pursues its efforts to address the challenge of cross-border fraud, it is important not to lose sight of the important work that must still be done in the United States to safeguard the interests of consumers. ***This Committee should hold hearings that includes consumer groups and approve legislation that safeguards the privacy of U.S. consumers in the 116th Congress.***

We ask that this letter and the attachments be entered in the hearing record.

Sincerely,

Marc Rotenberg
Marc Rotenberg
EPIC President

Caitriona Fitzgerald
Caitriona Fitzgerald
EPIC Policy Director

/s/ *Christine Bannan*
Christine Bannan
EPIC Consumer Protection Counsel

Attachments

EPIC, *Grading On A Curve* (2019).

Marc Rotenberg, *America Needs a Privacy Law*, New York Times (December 25, 2018)

Marc Rotenberg, After Latest Facebook Fiasco, Focus Falls on Federal Commission, Techonomy (December 21, 2018)

Marc Rotenberg, *Congress can follow the EU's lead and update US privacy laws,* Financial Times (June 1, 2018) ("Regarding innovation, it would be a critical mistake to assume that there a trade-off between invention and privacy protection. With more and more devices connected to the Internet, privacy and security have become paramount concerns. Properly understood, new privacy laws should spur the development of techniques that minimize the collection of personal data.")