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

November 21, 2019

Senator Kevin Thomas, Chair, Consumer Protection Committee
Senator Diane Savino, Chair, Internet and Technology Committee
New York State Senate
State Street and Washington Avenue
Albany, NY 12224

Dear Chair Thomas and Chair Savino:

We write to you in regarding your hearing on "Protecting Consumer Data and Privacy on Online Platforms"[1] We appreciate your attention to this issue. Consumers today face unprecedented risks of identity theft, financial fraud, and data breaches. States urgently need to pass data protection laws.

EPIC is a public interest research center established in 1994 to focus public attention on emerging privacy and civil liberties issues.[2] 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 Committees consider 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. Many now believe that the failure to establish a

[1] *Protecting Consumer Data and Privacy on Online Platforms,* N.Y. Sen. Committees on Consumer Protection and Internet Technology (Nov. 22, 2019), https://www.nysenate.gov/calendar/public-hearings/november-22-2019/public-hearing-protecting-consumer-data-and-privacy-0.
[2] *About EPIC*, EPIC (2019), https://www.epic.org/epic/about.html.
[3] *See* https://epic.org/GradingOnACurve/.

data protection agency in the U.S. has contributed to the growing incidents of data breach and identity theft.

A strong state privacy law would establish an independent state-level Data Protection Agency with resources, technical expertise, rulemaking authority and effective enforcement powers.

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

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.

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.[4]

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

Attachments

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

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