October 9, 2018

Senator John Thune, Chairman
Senator Bill Nelson, Ranking Member
U.S. Senate Committee on Commerce, Science, & Transportation
Russell Senate Office Building, Room 253
Washington, DC 20002

Dear Chairman Thune and Ranking Member Nelson:

We submit the following draft data protection framework on behalf of the dozen undersigned consumer and privacy organizations. We request that this statement be entered into the hearing record for "Consumer Data Privacy: Examining Lessons from the European Union's General Data Protection Regulation and the California Consumer Privacy Act."

The Framework outlines just some of the many issues that should be addressed to implement effective baseline privacy protections in the United States. We look forward to working with this committee and Congress to that end.

Sincerely,

Campaign for a Commercial-Free Childhood
Center for Digital Democracy
Constitutional Alliance
Consumer Action
Consumer Federation of America
Customer Commons
Cyber Privacy Project
Defending Rights & Dissent
Electronic Privacy Information Center
Privacy Times
U.S. Public Interest Research Group
World Privacy Forum

Draft Framework for Data Protection in the United States

From

Consumer and Privacy Organizations

(Fall 2018)

Enact Baseline Federal Data Protection Legislation

Our consumer and privacy organizations favor federal baseline legislation that ensures a basic level of protection for all individuals in the United States and oppose federal legislation that preempts stronger state laws. The states are the "laboratories of democracy" and have led the way in the development of innovative privacy legislation. US privacy laws typically establish a floor and not a ceiling. That is still the right approach, particularly as new challenges rapidly emerge.

Baseline federal legislation should be based on familiar Fair Information Practices, such as the widely followed OECD Privacy Guidelines. This framework creates obligations for companies that collect personal data, and rights for individuals whose personal data is collected. Core principles include: user control, transparency about business practices, collection and use limitations, data minimization and deletion, and security. "Personal data" should be broadly defined to include information that identifies, or could identify, a particular person.

Limit Government Access to Personal Data

Personal data held by companies is often sought by government agencies for law enforcement purposes. We do not object to the disclosure of specific records that are required for legitimate criminal investigations and obtained through an appropriate judicial procedure. However, there should be a clear standard in a privacy law for such disclosure. US companies should not disclose user data in bulk to the government agencies, particularly after the recent *Carpenter* ruling that established that individuals have a constitutional privacy interest in the personal data held by third parties.

Establish Algorithmic Transparency and End Discriminatory Profiling

Concerns about the fairness of automated decision-making are mounting as they are used to determine eligibility for jobs, housing, credit, insurance, and other necessities of life. Companies also use algorithms to target content and ads that

relate to critical opportunities. Bias and discrimination are often embedded in these systems, yet these algorithms are opaque and there is no accountability for their use. Algorithmic transparency, to promote fairness and to remove bias, is now a core element of modern privacy law and should be included in US privacy law.

Prohibit "Take it or Leave it" and Other Unfair Terms

Individuals cannot have meaningful control of their personal data if the terms of service require them to waive their privacy rights. Furthermore, requiring individuals to pay more or providing them with lower quality goods or services if they do not agree to waive their privacy rights is unfair and discriminates against those with less means.

Ensure Robust Enforcement

Robust enforcement is critical for effective privacy protection. Among the most serious risks facing consumers today are the ongoing breaches of personal data that contribute to identity theft, financial fraud, and many non-economic harms. But consumers typically receive only notification of breaches and time-limited credit monitoring services. And arbitration clauses do not protect consumer interests. Companies should be required by law to implement and maintain robust security measures. Furthermore, consumers should be able to pursue a private right of action that produces meaningful penalties. Statutory damages for violations of privacy obligations is an essential element of an effective privacy law. Robust enforcement also requires independent authority for State Attorneys General.

Promote Privacy Innovation

Our consumer and privacy organizations strongly favor innovative approaches to data protection, including strong encryption, robust techniques for deidentification and anonymization, and privacy enhancing techniques that minimize or eliminate the collection of personal data. Federal privacy law should make privacy innovation an affirmative obligation for all companies that collect and use personal data.

Establish a Data Protection Agency

The Federal Trade Commission helps to safeguard consumers and to promote competition, but the FTC is not an effective data protection agency. The FTC lacks rulemaking authority. Moreover, the agency lacks authority to enforce basic data protection obligations and has failed to enforce the orders it has established. Many democratic nations around the world have dedicated data protection agencies with strong authority and enforcement capabilities. The US needs a federal agency focused primarily on identifying emerging privacy challenges, ensuring compliance with data protection obligation and identifying emerging privacy challenges.