The Honorable Roger Wicker
Chairman
U.S. Senate Committee on Commerce, Science, & Transportation

The Honorable Maria Cantwell
Ranking Member
U.S. Senate Committee on Commerce, Science, & Transportation

September 22, 2020

Dear Senators Wicker and Cantwell:

The undersigned public interest groups have advocated for strong privacy legislation for many years. We thank the chairman for acknowledging the need for comprehensive federal privacy legislation and for the opportunity to comment on today's hearing, *Revisiting the Need for Federal Privacy Legislation*.[1] The COVID-19 pandemic has highlighted how essential the internet is to daily life and the pressing need for comprehensive privacy legislation. However, we do not believe the Setting an American Framework to Ensure Data Access, Transparency, and Accountability Act (SAFE DATA Act)[2] will adequately protect privacy in the United States.

In November 2018, many of our groups argued that federal privacy legislation should center on four principles to serve the public interest.[3] While the SAFE DATA Act would be a slight improvement on the status quo, it fails to fulfill these principles.

(1) Privacy protections must be strong, meaningful, and comprehensive, with a focus on implementing Fair Information Practices (FIPs).

The bill lacks adequate corporate obligations to prevent the invasive tracking of internet users and lacks provisions that give users meaningful control over their personal data and how that data is used. Rather than prohibiting harmful uses of data, the bill is still overly reliant on a "notice and consent" model that is based on transparency rather than strong user rights. For example, the bill's data minimization provision is not a true reflection of the FIP because it would only prohibit companies from collecting more data than is "reasonably necessary" to the purposes specified in privacy policies, and therefore would not actually limit data collection. Additionally, the SAFE DATA Act allows for "approved certification programs" (also known as "safe harbors"), which may allow the largest companies to write their own compliance regimes, likely amounting to little more than ineffective self-regulation.

(2) Data practices must protect civil rights, prevent discrimination, and advance equal opportunity.

The bill does not protect civil rights—it merely grants the Federal Trade Commission (FTC) a supporting role to work with other agencies, which the FTC can already do, and requires the FTC to report annually to Congress and conduct two studies on algorithmic bias within eight years. Given the growing mountain of evidence of data being used in a discriminatory fashion to deny protected classes critical opportunities, the lack of any meaningful protections are unacceptable.

---

[1] "Revisiting the Need for Federal Privacy Legislation." U.S. Senate Committee on Commerce, Science, & Transportation Hearing. 23 September 2020. https://www.commerce.senate.gov/2020/9/revisiting-the-need-for-federal-data-privacy-legislation.

[2] "Wicker, Thune, Fischer, Blackburn Introduce Consumer Data Privacy Legislation." 17 September 2020. https://www.commerce.senate.gov/2020/9/wicker-thune-fischer-blackburn-introduce-consumer-data-privacy-legislation.

[3] "Principles for Privacy Legislation." Open Technology Institute, New America Foundation. 13 November 2018. https://www.newamerica.org/oti/press-releases/principles-privacy-legislation/.

(3) Governments at all levels should play a role in protecting and enforcing privacy rights.

The bill includes an extremely broad preemption provision that would remove state legislatures completely from protecting privacy, which would have the effect of nullifying state consumer protection and civil rights laws as they relate to the sharing or use of personal information. This includes many state student and employee privacy laws where the bill offers no new protections, and in fact explicitly excludes employee data from its protections. State laws including the California Consumer Privacy Act, Illinois Biometric Information Privacy Act, and Maine Broadband Service Provider Privacy Act are stronger than the SAFE DATA Act and would be preempted by it. The enforcement authorities are also insufficient because, while we are pleased to see the provision allowing for enforcement by state attorneys general, the bill would not significantly improve the enforcement powers of the FTC and would not empower individuals to vindicate their rights in court.

(4) Legislation should provide redress for privacy violations beyond those causing financial harm, and should recognize and include intangible harms.

The bill envisions privacy harms as a matter of non-disclosure, but this is a fundamental misunderstanding of privacy harms. Beyond obvious financial harms like identity theft, privacy violations can lead to many types of harms, including but not limited to emotional or reputational harm, limiting awareness of and access to opportunities, discrimination against protected classes, informational disparities causing unfair price discrimination, and the erosion of trust and freedom of expression in society.

For the above reasons, the undersigned groups oppose the SAFE DATA Act. We will continue to support the bipartisan efforts of the Committee to craft strong legislation that recognizes the privacy needs of Americans, protects them from data-driven discrimination, and places the onus of protecting privacy primarily on companies, not individuals.

Signed,

Access Now
American Association for Justice
Campaign for a Commercial-Free Childhood
Center for Digital Democracy
Color of Change
Common Cause
Constitutional Alliance
Consumer Action
Consumer Federation of America
Fight for the Future
Free Press Action
Media Alliance
National Hispanic Media Coalition
National Workrights Institute
New America's Open Technology Institute
Parent Coalition for Student Privacy
Privacy Rights Clearinghouse
Public Citizen
Public Knowledge
U.S. PIRG