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

July 26, 2022

The Honorable Maria Cantwell, Chair
The Honorable Roger Wicker, Ranking Member
U.S. Senate Committee on Commerce, Science, and Transportation
512 Dirksen Senate Office Building
Washington, DC 20510

Dear Chair Cantwell and Ranking Member Wicker:

Thank you for considering S. 1628, Children and Teens' Online Privacy Protection Act and S. 3663, the Kids Online Safety Act. EPIC has long advocated for protecting children's online privacy and played a leading role in both the drafting of the Children's Online Privacy Protection Act (COPPA) and developing the authority of the Federal Trade Commission to address emerging children's' privacy issues.[1]

But all Americans, young and old, deserve privacy. Privacy is a fundamental right, and it is long past time for Congress to act to protect the privacy rights of all Americans. While we commend this Committee's work on children's privacy, the best way to protect the privacy rights of children, teens, and adults would be to consider the American Data Privacy and Protection Act ("ADPPA") as amended and reported favorably out of the House Energy & Commerce Committee last week. ADPPA establishes critical protections for all Americans and makes much needed advancements for privacy rights at a time when those rights are very much at risk. We urge you to schedule ADPPA for a markup as soon as possible.

Below we highlight the most crucial provisions of ADPPA, including data minimization, enhanced protections for children and teens, civil rights protections, and enforcement mechanisms.

Data Minimization is Critical in Limiting Unfettered Data Collection

EPIC is particularly encouraged by the ADPPA's focus on data minimization. Section 101 of the ADPPA establishes limits on the unfettered processing of personal data by requiring that entities only collect, use, and transfer data that is reasonably necessary and proportionate to provide a specific product or service requested by the individual with some exceptions specifically enumerated

[1] *See Children's Privacy Protection and Parental Empowerment Act: H.R. 3508*, H. Comm. on the Judiciary, Subcomm. on Crime, 104th Cong (1996), (statement of Marc Rotenberg, Executive Director, EPIC), available at https://archive.epic.org/privacy/kids/EPIC_Testimony.html; EPIC, *EPIC Letter to Christine Varney on Direct Marketing Use of Children's Data* (December 14, 1995), available at http://archive.epic.org/privacy/internet/ftc/ftc_letter.html; Comments of EPIC, *Agency Information Collection Activities; Proposed Collection; Comment Request*, File No. 49557 (Dec. 3, 2018), https://epic.org/apa/comments/EPIC-FTC-COPPA-Dec2018.pdf; Comments of EPIC, *Children's Online Privacy Protection Act Rule Review*, Project No. P104503 (Sept. 24, 2012), https://epic.org/privacy/kids/EPIC-COPPA-2012-Rule-Rev-Cmts.pdf; EPIC, *Children's Privacy,* https://epic.org/issues/data-protection/childrens-privacy/.

in the bill. The baseline requirement to minimize data collection and use is what sets ADPPA apart from the notice-and-choice regimes of the past. It takes the onus off individuals and instead requires companies to limit data collection and better align their data practices with what consumers expect.

ADPPA also rightly recognizes that some sensitive categories and uses of data deserve stricter controls. It sets strong restrictions on the collection and use of sensitive data, including precise geolocation, biometric, and health information, as well as data identifying an individual's online activities over time and across third party websites and online services. Companies may only collect and use these types of data if doing so is strictly necessary and may not transfer such data to third parties without the individual's affirmative express consent. The ADPPA prohibits the use of sensitive data for targeted advertising purposes. EPIC believes that these protections directly limit the most harmful business practices that a privacy law is intended to address.

Enhanced Protections for Children and Teens

The American Data Privacy and Protection Act includes many of the enhanced protections for children and teens that are included in S. 1628, and in many cases are stronger. First, all covered data of individuals under the age of 17 is considered sensitive data and therefore the collection and use of minors' data is strictly regulated as described above, including a prohibition on the transfer of minors' data without the express opt-in permission from their parents or guardians. Targeted advertising to individuals under 17 is expressly prohibited. Like S. 1628, ADPPA establishes a Youth Privacy and Marketing Division at the FTC. Algorithmic impact assessments required under the bill must assess and mitigate harms to kids and teens. ADPPA would accomplish the Committee's goals of protecting children and teens online while also protecting adults.

Civil Rights Protections and Algorithmic Oversight

Critically, ADPPA would extend civil rights protections online and provide oversight of the use of algorithms that may cause harm. The use of artificial intelligence and other automated systems to make decisions about individuals poses significant risks to fundamental rights. Public and private actors are increasingly relying on automated decision-making tools to determine eligibility for jobs, education, housing, parole, bail, credit, insurance, healthcare, and government services. The error, bias, and discriminatory patterns embedded in these systems perpetuate systemic inequality, yet, under current law, companies are not required to evaluate the impacts and biases of these systems before they use them.

The American Data Privacy and Protection Act sets accountability and transparency requirements for automated decision-making tools by requiring Algorithmic Impact Assessments and Algorithm Design Evaluations, which can provide meaningful oversight if done right.

ADPPA's Three-Tier Enforcement Structure is Critical

As with any law establishing new rights, a framework for robust enforcement is critical to the success of a comprehensive privacy regime. The ADPPA's three-tier enforcement structure sets it apart from other privacy laws. One of the biggest criticisms of the European Union's General Data Protection Regulation (GDPR) is that it is not adequately enforced. When enforcement is left to individual states, and further limited to states where a company facing an enforcement action is

headquartered, there are not adequate resources to ensure compliance. The ADPPA aims to avoid this issue by instead empowering enforcement authorities at the federal, state, and individual level.

At the federal level, EPIC has long advocated for the creation of a standalone Data Protection Agency. ADPPA would not go quite so far, but it would establish a new privacy bureau within the Federal Trade Commission. This is a step in the right direction provided Congress allocates adequate resources to the new bureau for the FTC to carry out all the regulatory and enforcement obligations required under the bill.

At the state level, Attorneys General play a critical role in ensuring that privacy rules are enforced, and their investigations benefit from their long history in the consumer watchdog role. The American Data Privacy and Protection Act rightly preserves this role and expands state enforcement of the new federal regime, including by state consumer protection agencies. EPIC believes that it is essential for the ADPPA to empower state consumer protection agencies, like the California Privacy Protection Agency, to ensure that individual privacy rights are robustly enforced.

Critically, the ADPPA also provides enforcement of key sections through a private right of action to ensure that there is a backstop in cases where the federal and state agencies don't take on the enforcement role.

Preemption of State Privacy Laws

EPIC has long argued that federal privacy laws should set a floor, allowing states to enact stronger protections. We still believe this is the best approach and would prefer that the ADPPA took that approach, but we recognize that compromise was necessary to enact a national standard that would protect the privacy of all Americans. A national standard is important—as it stands today, individuals in California and Colorado have privacy rights online that the vast majority of Americans do not. EPIC believes that the provisions of the ADPPA are as strong or stronger than the standards set by current state privacy laws. And we will continue to advocate for the highest level of protections for all Americans' data regardless of the size or nature of the entities involved.

This is not a perfect privacy bill, but EPIC believes that the ADPPA would establish strong protections for Americans' privacy and deserves to be considered by the Senate Commerce Committee. This is just the start of the process towards restoring privacy for Americans. The bipartisan American Data Privacy and Protection Act presents Congress with the best opportunity it has had in decades to stem the very real data abuses and privacy harms that are happening online every minute of every day due to the lack of a U.S. privacy law. EPIC urges the Committee to schedule ADPPA for a markup as soon as possible and keep moving this process forward. Americans of all ages deserve privacy and civil rights online.

Sincerely,

Alan Butler
EPIC Executive Director

Caitriona Fitzgerald
EPIC Deputy Director