

July 19, 2022

The Honorable Frank Pallone, Chair
The Honorable Cathy McMorris Rogers, Ranking Member
House Committee on Energy & Commerce
Washington, DC 20515

Dear Chair Pallone, Ranking Member McMorris Rogers, and Members of the Committee:

EPIC writes in support of the Amendment in Nature of a Substitute to the American Data Privacy and Protection Act filed today (“the Amended Bill”). EPIC has been calling on Congress to pass a comprehensive privacy law for more than 20 years. We commend your work in crafting federal privacy legislation that would establish critical protections for Americans and make much needed advancements for privacy rights at a time when those rights are very much at risk. We appreciate the opportunities EPIC has been provided to give input on the bill, including testifying before the Consumer Protection Subcommittee last month. As we told the Subcommittee then, privacy is a fundamental right, and it is long past time for Congress to act to protect the privacy rights of all Americans. We appreciate the Committee’s work towards this goal and urge your approval of the Amended Bill.

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 Amended Bill 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 in the bill. The baseline requirement to minimize data collection and use is what sets this bill 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.

The American Data Privacy and Protection Act also rightly recognizes that some sensitive categories and uses of data deserve stricter controls. The Amended Bill 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 this law is intended to address.

It is, however, absolutely critical that this bill cover the full range of entities and service providers that process personal data, and we urge the Committee to restore those provisions (previously found in Section 302 of the bill) during markup. It is equally important that entities acting on behalf of the government, such as ed tech providers and law enforcement service providers, be required to comply with privacy rules. The service provider and third-party provisions should be restored and amended to include service providers and third parties acting under contract with government entities.

Civil Rights Protections and Algorithmic Oversight

Critically, the Amended Bill 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, neither public agencies nor private companies are typically 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. We commend the Committee for adding specific requirements for what companies must include in impact assessments. While this section could be made stronger by requiring the use of an independent auditor and public transparency, it is certainly a step in the right direction.

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. The Amended Bill 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. We are happy to continue to work with the Committee to ensure that the bill accomplishes that goal.

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. We commend the Committee leaders for their hard work in ensuring this additional protection for individuals who have been the victims of data abuse.

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 the support of the 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 support the Amended Bill and keep moving this process forward. We need comprehensive data protection legislation, robust enforcement, and ample resources to ensure privacy, equality, and security in our online world.

Sincerely,

Alan Butler
EPIC Executive Director

Caitriona Fitzgerald
EPIC Deputy Director