ICLE tl;dr

American Data Privacy and Protection Act

June 2022

tl;dr

Background: After years of fragmented privacy law across the 50 states, a recently introduced bipartisan and bicameral bill proposes to create a federal privacy regime. Sponsors of the American Data Privacy and Protection Act (ADPPA) say it will set a national baseline for privacy protections and user remedies, while allowing firms to continue to innovate.

But... the bill's breadth and onerous requirements could have unintended negative consequences for consumers. Worse, the measure would only partially preempt state law, arguably leaving the worst of both worlds.

KEY TAKEAWAYS

THE BILL'S DEFINITIONS ARE OVERLY BROAD

The ADPPA sets expansive definitions for both the firms and the types of data it covers. The bill implicates essentially all personal data and effectively any firm subject to the jurisdiction of the Federal Trade Commission (FTC) or acting as a common carrier.

The bill does not adequately distinguish "controllers" and "processors" of data, thus placing the same onerous obligations on firms irrespective of their role. Despite some attempts to tailor the burdens it imposes, it would apply to firms of all sizes, raising the concern that even the smallest firms might need to employ data-privacy experts to ensure compliance.

The bill focuses on "covered data" that identifies, is linked to, or is "reasonably linkable" to an individual or a device. It lays out heightened requirements for "sensitive" covered data, an expansive category that includes any geolocation information and "information revealing online activities over time." Affirmative consent would be required to collect and use "sensitive" data, fundamentally constricting digital commerce as we know it.

THE ADPPA IMPOSES ONEROUS OBLIGATIONS THAT ARE NOT ADEQUATELY TAILORED

Among the myriad obligations the bill imposes on covered entities is an expansive data-minimization requirement to bar the "unnecessary" collection or use of covered data. This provision is even more onerous than the EU GDPR's parallel requirement, because the legal bases for collection are narrower.

The bill classifies all data on individuals under age 17 as "sensitive," and precludes all targeted advertising toward those users. But age verification is notoriously difficult online. While the current draft imposes obligations on firms with "actual" knowledge that an individual is under age 17, these requirements still present near limitless potential for liability.

UNDERBAKED THEORIES OF DISCRIMINATION

Like the previously introduced Algorithmic Accountability Act, the ADPPA proposes

sweeping obligations for "large data holders," including that they conduct "algorithmic impact assessments" in order to mitigate "algorithmic harms" from essentially any kind of software. This would require large firms to assess the potential for "disparate impact" on protected classes of users. Conducting such assessments is a fraught exercise, since expansive theories of harm can have a chilling effect on novel uses of data. By effectively imposing "prior approval" on algorithms, the bill would increase the cost, complexity, and time associated with product development.

RIGHTS AND ENFORCEMENT ISSUES

The ADPPA delegates enforcement authority both to state attorneys general and to the FTC, which could pursue action against violations as "unfair or deceptive acts or practices" (UDAP). It also would create a private right of action (PRA) allowing individuals to seek damages and attorneys fees for violations, after giving notice to the FTC and relevant state AG.

The legislation also details broad rights that individuals could exercise against firms that collect data, including rights to prevent collection, to request collected data, and to request correction or deletion of that data.

In practice, the FTC will determine the scope of enforcement, as it will set standards for the types of "reasonably necessary, proportionate, and limited" data collection in which covered entities may engage. The commission also would have rulemaking authority to define new categories of "sensitive" data. Given the incredible variety of firms, users, and data uses that the ADPPA would cover, adopting narrow interpretations of what data counts as "reasonably necessary" could threaten to hamper innovation.

LIMITED PREEMPTION OF STATE PRIVACY LAW

A major reason that many covered firms have sought a national privacy standard is to provide clarity amid a patchwork of state-by-state standards.

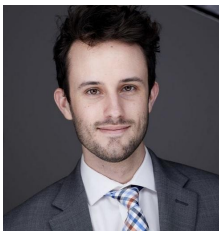
The ADPPA, however, offers only very weak preemption. The bill carves out numerous categories of state law that would be excluded from preemption—including those covering civil rights, employee rights, consumer protection, and tort and contract law—as well as several specific state laws that would be explicitly excluded, including Illinois' Genetic Information Privacy Act and elements of the California Consumer Privacy Act.

These broad carve-outs practically ensure that ADPPA will not create a uniform and workable system, and could potentially render the entire preemption section a dead letter. As written, it offers the worst of both worlds: a very strict federal baseline that also permits states to experiment with additional data-privacy laws.

For more on state consumer privacy laws, see "Guiding Principles and a Legislative Checklist for Consumer Privacy Regulation," published jointly by ICLE and the Reason Foundation.

CONTACT US

Kristian Stout
Director of
Innovation Policy
kstout@laweconcenter.org



Spencer Kahn
Nonresident Research
Associate
spencer.j.kahn@gmail.com

ICLE International Center for Law & Economics