Congressional Research Service
Informing the legislative debate since 1914

Legal Sidebar

Overview of the American Data Privacy and Protection Act, H.R. 8152

June 30, 2022

On June 21, 2022, the House Energy and Commerce Committee introduced the American Data Privacy and Protection Act (ADPPA), H.R. 8152, which would create a comprehensive federal consumer privacy framework. Some commentators have noted the bill's novel compromises on two issues—whether to preempt state privacy laws and whether to create a private right of action—that have impeded previous attempts to create a national privacy framework.

The bipartisan bill is co-sponsored by House Energy and Commerce Committee Chairman Frank Pallone, Jr. and Ranking Member Cathy McMorris Rogers and promoted in the Senate by Senate Commerce Committee Ranking Member Roger Wicker. In a joint statement, Representatives Pallone and McMorris Rodgers and Senator Wicker described the bill as "strik[ing] a meaningful balance" on key issues. Senate Commerce Committee Chair Maria Cantwell, however, has critiqued the ADPPA as having "major enforcement holes," prompting other commentators to question whether the Senate will pass the bill. Members of the House Energy and Commerce Committee raised additional concerns during a markup hearing on June 23, 2022. Still, some scholars are hopeful that Congress will pass the bill.

This Sidebar first provides a summary of the ADDPA. It then compares several of the bill's key provisions to other privacy bills from the 117th and 116th Congresses before examining some considerations for Congress, including potential next steps for the legislation.

Summary of the Bill

The ADPPA would govern how companies across different industries treat consumer data. While not an exhaustive summary, some key facets of the bill are as follows:

- ***Covered Entities***. It would apply to most entities, including nonprofits and common carriers. Some entities, such as those defined as *large data holders* that meet certain thresholds or *service providers* that use data on behalf of other covered entities, would face different or additional requirements.
- ***Covered Data.*** It would apply to information that "identifies or is linked or reasonably linkable" to an individual.

Congressional Research Service
https://crsreports.congress.gov
LSB10776

- ***Duties of Loyalty.*** It would impose several duties on covered entities, including requirements to abide by data minimization principles and special protections for certain types of data, such as geolocation information, biometric information, and nonconsensual intimate images.
- ***Transparency.*** It would require covered entities to disclose, among other things, the type of data they collect, what they use it for, how long they retain it, and whether they make the data accessible to the People's Republic of China, Russia, Iran, or North Korea.
- ***Consumer Control and Consent.*** It would give consumers various rights over covered data, including the right to access, correct, and delete their data held by a particular covered entity. It would require covered entities to get a consumer's affirmative, express consent before using their "sensitive covered data" (defined by a list of sixteen different categories of data). It would further require covered entities to give consumers an opportunity to object before the entity transfers their data to a third party or targets advertising toward them.
- ***Youth Protections.*** It would create additional data protections for individuals under the age of 17, including a prohibition on targeted advertising, and it would establish a Youth Privacy and Marketing Division at the Federal Trade Commission (FTC).
- ***Third-Party Collecting Entities.*** It would create specific obligations for third-party collecting entities, which are entities whose main source of revenue comes from processing or transferring data that it does not directly collect from consumers (e.g., data brokers). These entities would have to comply with FTC auditing regulations and, if they collect data above the threshold amount of individuals or devices, would have to register with the FTC.
- ***Civil Rights and Algorithms.*** It would prohibit most covered entities from using covered data in a way that discriminates on the basis of protected characteristics (such as race, gender, or sexual orientation). It would also require large data holders to conduct algorithm impact assessments. These assessments would need to describe the entity's steps to mitigate potential harms resulting from its algorithms, among other requirements. Large data holders would be required to submit these assessments to the FTC and make them available to Congress on request.
- ***Data Security:*** It would require covered entities to adopt data security practices and procedures that are reasonable in light of their size and activities. It would authorize the FTC to issue regulations elaborating on these data security requirements.
- ***Small- and Medium-size Businesses:*** It would also relieve small- and medium-size businesses from complying with several requirements; for instance, these businesses may respond to a consumer's request to correct their data by deleting the data, rather than correcting it.
- ***Enforcement.*** It would be enforceable by the FTC, under that agency's existing enforcement authorities, and by state attorneys general in civil actions.
- ***Private right of action.*** It would create a delayed private right of action starting four years after the law's enactment. Injured individuals would be able to sue covered entities in federal court for damages, injunctions, litigation costs, and attorneys' fees. Individuals would have to notify the FTC or their state attorney general before bringing suit. Before bringing a suit for injunctive relief or a suit against a small- or medium-size business, individuals would be required to give the violator an opportunity to address the violation.
- ***Preemption.*** It would generally preempt any state laws that are "covered by the provisions" of the ADPPA or its regulations, although it would expressly preserve sixteen

different categories of state laws, including consumer protection laws of general applicability and data breach notification laws. It would also preserve several specific state laws, such as Illinois' Biometric Information Privacy Act and Genetic Information Privacy Act and California's private right of action for victims of data breaches.

Comparison to Other Privacy Legislation

The ADPPA is, in many ways, similar to a number of other consumer privacy bills introduced in the 116th and 117th Congresses. It differs, however, from earlier bills in a key way: it both contains a private right of action and generally preempts state laws, including comprehensive privacy laws enacted by California, Colorado, Connecticut, Utah, and Virginia. In addition, the ADDPA does not include a blanket restriction on engaging in "harmful" data practices to the detriment of end users, in contrast to the "duty of loyalty" contained in Senator Cantwell's Consumer Online Privacy Rights Act (COPRA), S. 3195, or Senator Brian Schatz's Data Care Act of 2021, S. 919.

Tables 1 and 2 compare the ADDPA to the following bills from the 117th Congress:

- COPRA;
- The Data Care Act of 2021;
- The Online Privacy Act of 2021 (OPA), H.R. 6027; and
- The Control Our Data Act (CODA), a discussion draft released by the Republican members of the House Energy and Commerce Committee in November 2021.

Table 1 examines the individual rights and obligations created by each bill, while **Table 2** compares the bills' enforcement mechanisms and whether each bill would preempt state privacy laws. For more information on versions of COPRA and the OPA introduced in the 116th Congress, see CRS Legal Sidebar LSB10441, *Watching the Watchers: A Comparison of Privacy Bills in the 116th Congress*.

Table 1. Comparison of Enforcement Mechanisms and Preemption

	ADPPA	COPRA	Data Care Act	OPA	CODA
Enforcement					
Federal Agency Enforcement	FTC (§ 401)	FTC (§ 301(a))	FTC (§ 4(a))	New Digital Privacy Agency (Tits. III and IV)	FTC (§ 113(a))
State Attorneys General	Yes (§ 402)	Yes (§ 301(b))	Yes (§ 4(b))	Yes (§ 404)	Yes (§ 113(b))
Private Right of Action	Yes, with four-year phase-in (§ 403)	Yes (§ 301(c))	Silent	Yes (§ 405)	No (§ 113(f))
State Law Preemption	Yes, with exceptions (§ 404(b))	Yes, if state laws afford less protection ((§ 302(c))	No (§ 6(1))	Silent	Yes (§ 112(a))

Source: CRS, based on information in the ADDPA, COPRA, Data Care Act, OPA, and CODA.

Table 2. Comparison of Rights and Obligations

	ADPPA	COPRA	Data Care Act	OPA	CODA
Individual Rights					

	ADPPA	COPRA	Data Care Act	OPA	CODA
Access	§ 203(a)(1)	§ 102(a)	Silent	§ 101	§ 102(c)(1)(B)
Correction	§ 203(a)(2)	§ 104	Silent	§ 102	§ 102(c)(1)(C)
Deletion	§ 203(a)(3)	§ 103	Silent	§ 103	§ 102(c)(1)(D)
Opt Out	§ 204	§ 105(b)	Silent	§ 208(b)	§ 102(c)(1)(E)
Portability	§ 203(a)(4)	§ 105(a)	Silent	§ 104	Silent
Obligations					
Notice	§ 202(e)	§ 102(b)	Silent	§ 210	§ 102(b)
Affirmative Consent for Sensitive Info.	§ 102(a)(3)(A)	§ 105(c)	Silent	§ 210	§ 103
Privacy Policy	§ 202(a)	§ 102(b)	Silent	§ 211	§ 102(a)
Minimization	§ 101	§ 106	Silent	§§ 201–202	§§ 104–105
Data Security	§ 208	§ 107	§ 3(b)(1)(A)	§ 212	§ 109
Breach Notices	Silent	Silent	§ 3(b)(1)(B)	§ 213	Silent

Source: CRS, based on information in the ADPPA, COPRA, Data Care Act, OPA, and CODA.

Next Steps

The ADPPA has bipartisan support, but some Members of Congress have raised concerns with the bill. Senators Cantwell and Schatz have both criticized the bill's failure to impose a "duty of loyalty" on covered entities. While the ADPPA has various requirements that are classified under a "Duty of Loyalty" heading, these requirements differ from those included in COPRA or the Data Care Act. COPRA's "duty of loyalty" would prohibit businesses from engaging in "harmful" data practices, which the bill defines to mean using covered data "in a manner that causes or is likely to cause" injury to the subject of the covered data. The Data Care Act's "duty of loyalty" would prohibit covered providers from using data in a way that would "benefit the [provider] to the detriment of the end user" and would "result in reasonably foreseeable and material physical harm" or "be unexpected and highly offensive" to the end user. The ADPPA's "Duty of Loyalty" defines several specific prohibited data practices, but does not broadly prohibit providers from acting in ways that could harm individuals.

Various concerns were also raised by members in the ADPPA's markup on June 23, 2022, by the House Subcommittee on Consumer Protection and Commerce. These questions included whether the youth-protection provisions should be strengthened; whether the current bill would force businesses to eliminate customer loyalty programs; whether the research exemption should be amended to address healthcare research and research into social media platforms; whether the bill should address politically biased algorithms; whether the preemption provision is sufficiently clear; whether the bill should clarify if the FTC, state attorneys general, and private litigants may all bring suits for the same conduct; and whether the right to cure violations (which applies only to businesses of a certain size in the current draft) should be expanded to all enforcement actions. While the subcommittee voted to move the bill to the full House Energy and Commerce Committee, Committee Chairman Frank Pallone and Subcommittee Chairwoman Janice Schakowsky indicated that the bill would continue to be negotiated and finalized. Consequently, the ADPPA may continue to evolve.

Author Information

Jonathan M. Gaffney
Legislative Attorney

Chris D. Linebaugh
Legislative Attorney

Eric N. Holmes
Legislative Attorney

Disclaimer