

Overview of the American Data Privacy and Protection Act, HR 8152



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

Updated August 31, 2022

On July 20, 2022, the House Energy and Commerce Committee [voted 53-2 to advance](#) the [American Data Privacy and Protection Act \(ADPPA\)](#), H.R. 8152, to the full House of Representatives. The ADPPA would create a comprehensive federal consumer privacy framework. Some commentators [have noted](#) the bill's novel compromises on two issues that [have impeded](#) previous attempts to create a national privacy framework: whether to preempt state privacy laws and whether to create a private right of action.

The bipartisan bill is co-sponsored by House Energy and Commerce Committee Chairman Frank Pallone, Jr. and Ranking Member Cathy McMorris Rogers, and is promoted in the Senate by 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 [has critiqued](#) the ADPPA as having “major enforcement holes,” prompting other commentators [to question](#) whether the Senate will pass the bill.

This Sidebar first provides a summary of the version of the ADPPA ordered to be reported by the House Commerce Committee on July 20. 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.

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.** The bill would [apply](#) to most entities, including nonprofits and common carriers. Some entities, such as those defined as [large data holders](#) that meet certain thresholds and [service providers](#) that use data on behalf of other entities (including covered entities, government entities, and other service providers), would face different or additional requirements.
- **Covered Data.** The bill 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.*** The bill would [prohibit](#) covered entities from collecting, using, or transferring covered data beyond what is reasonably necessary and proportionate to provide a service requested by the individual, unless the collection, use, or disclosure would fall under one of seventeen permissible purposes. It also would create special protections for certain types of [sensitive covered data](#), defined as sixteen different categories of data. Among other things, the bill would [require](#) covered entities to get a consumer’s affirmative, express consent before transferring their sensitive covered data to a third party, unless a specific exception applies.
 - ***Transparency.*** The bill 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.*** The bill 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 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.*** The bill would [create](#) additional data protections for individuals under age 17, including a prohibition on targeted advertising, and it would establish a Youth Privacy and Marketing Division at the Federal Trade Commission (FTC). These additional protections would only apply when the covered entity knows the individual in question is under age 17, though certain social media companies or large data holders would be deemed to “know” an individual’s age in more circumstances.
 - ***Third-Party Collecting Entities.*** The bill would create specific obligations for [third-party collecting entities](#), which are entities whose main source of revenue comes from processing or transferring data that they do 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. The FTC would establish a searchable registry of third-party collecting entities and a “Do Not Collect” mechanism by which individuals could request that all registered entities refrain from collecting covered data relating to the individual.
 - ***Civil Rights and Algorithms.*** The bill would [prohibit](#) most covered entities from using covered data in a way that discriminates on the basis of protected characteristics (such as race or sex). 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. The bill would require large data holders to submit these assessments to the FTC and make them available to Congress on request.
 - ***Data Security.*** The bill would [require](#) a covered entity to adopt data security practices and procedures that are reasonable in light of the entity’s size and activities. It would [authorize](#) the FTC to issue regulations elaborating on these data security requirements.
 - ***Small- and Medium-size Businesses.*** The bill would also [relieve](#) small- and medium-size businesses that meet certain size and data-collection thresholds 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, and are exempt from most of the bill’s data security requirements.
 - ***Enforcement.*** The bill would be [enforceable](#) by the FTC, under the agency’s existing enforcement authorities, and by state attorneys general and state privacy authorities in
-

civil actions. The bill also would [give](#) the California Privacy Protection Agency authority to enforce the ADPPA in the “same manner it would otherwise enforce” California’s privacy law, the California Consumer Privacy Act.

- **Private right of action.** The bill would [create](#) a delayed private right of action starting two years after the law’s enactment. Injured individuals, or classes of 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. The bill also would render pre-dispute arbitration agreements or joint-action waivers with individuals under the age of 18 unenforceable in disputes arising under the ADPPA.
- **Preemption.** The bill 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 from earlier bills, however, in two key ways: 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 ADPPA 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 ADPPA 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 compares the bills’ enforcement mechanisms and whether each bill would preempt state privacy laws, while **Table 2** examines the individual rights and obligations created by each bill. 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))

	ADPPA	COPRA	Data Care Act	OPA	CODA
State Attorneys General	Yes (§ 402)	Yes (§ 301(b))	Yes (§ 4(b))	Yes (§ 404)	Yes (§ 113(b))
Private Right of Action	Yes, with two-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(I))	Silent	Yes (§ 112(a))

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

Table 2. Comparison of Rights and Obligations

	ADPPA	COPRA	Data Care Act	OPA	CODA
Individual Rights					
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.

Considerations for Congress

The ADPPA has bipartisan support, and various interest groups and commentators, such as the [Electronic Privacy Information Center](#), the [Center for Democracy & Technology](#), and the [Washington Post’s editorial board](#), have expressed enthusiasm for the bill. In an [August 25 letter](#) to House Speaker Nancy Pelosi, forty-eight different public interest groups urged Congress to move the ADPPA forward through Congress, stating that the bill is a “meaningful compromise” and that a failure to act may “forestall progress on this issue for years to come.” At the same time, some Members of Congress and other commentators have raised concerns with the bill. Senators Cantwell and Schatz, for example, 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" imposes a data minimization requirement and defines several specific prohibited data practices, but it does not broadly prohibit providers from acting in ways that could harm individuals.

Some have also raised concerns over the ADPPA's preemption provisions. The Attorney General of California sent Congress a [letter](#) co-signed by nine other state attorneys general criticizing the ADPPA because it would set a "ceiling" for privacy rights rather than a "floor." These state attorneys general argue that states should be allowed to adopt their own privacy laws so they can "legislate responsively" to changes in technology and practices. In the Commerce Committee's July 20 markup of the ADPPA, some Members [expressed similar concerns](#) over the ADPPA's preemption of state law. Other [Members](#) and [commentators](#) have pushed back on these criticisms, pointing to the strengths of the ADPPA's protections and the importance of setting a federal standard.

Author Information

Jonathan M. Gaffney
Legislative Attorney

Chris D. Linebaugh
Legislative Attorney

Eric N. Holmes
Legislative Attorney

Disclaimer

This document was prepared by the Congressional Research Service (CRS). CRS serves as nonpartisan shared staff to congressional committees and Members of Congress. It operates solely at the behest of and under the direction of Congress. Information in a CRS Report should not be relied upon for purposes other than public understanding of information that has been provided by CRS to Members of Congress in connection with CRS's institutional role. CRS Reports, as a work of the United States Government, are not subject to copyright protection in the United States. Any CRS Report may be reproduced and distributed in its entirety without permission from CRS. However, as a CRS Report may include copyrighted images or material from a third party, you may need to obtain the permission of the copyright holder if you wish to copy or otherwise use copyrighted material.