Congressional Research Service
Informing the legislative debate since 1914

Legal Sidebar

The American Privacy Rights Act

May 7, 2024

On April 7, 2024, Senate Commerce Committee Chair Maria Cantwell and House Energy and Commerce Committee Chair Cathy McMorris Rodgers jointly released a draft of the American Privacy Rights Act (APRA). The APRA would create a comprehensive federal consumer privacy framework. It builds on prior congressional efforts to enact a comprehensive privacy bill, most notably incorporating elements of the American Data Privacy and Protection Act (ADPPA) (H.R. 8152), which was advanced out of the House Energy and Commerce Committee during the 117th Congress.

This Sidebar provides a summary of the APRA, as released on April 7, 2024, and briefly compares it with the ADPPA and other comprehensive privacy bills that have been introduced in Congress. The Sidebar explains that the APRA borrows a substantial amount from the ADPPA but includes material differences, such as its treatment of small businesses, approach toward minors, algorithmic opt-out rights, effective availability of a private right of action, and interaction with state laws. The Sidebar concludes by discussing stakeholders' reaction to the APRA and potential litigation that may arise should the bill be enacted.

Summary of the Bill

Key Definitions

The APRA's chief focus is governing how covered entities use covered data. Thus, these two definitions are central to the bill's scope. The APRA defines "covered entities" to include most individuals, commercial entities, and nonprofits that "alone, or jointly with others, determine[] the purposes and means of collecting, processing, and retaining, or transferring covered data." Small businesses, among others, are exempt from this definition. The APRA defines "covered data" to include any information that "identifies or is linked or reasonably linkable" to an individual.

Another key definition is sensitive covered data, for which the APRA provides additional protections. "Sensitive covered data" includes, among other things, government-issued identifiers, genetic information, health information, financial information, precise geolocation information, and information about an individual under the age of 17. The APRA would give the Federal Trade Commission (FTC) authority to expand the categories of sensitive covered data through regulation.

Congressional Research Service
https://crsreports.congress.gov
LSB11161

The APRA also defines large data holder and data broker, which are two subsets of covered entities that must comply with additional requirements. Large data holders are those covered entities with annual gross revenue of more than $250 million in the preceding calendar year that collect enough data to meet one of the bill's thresholds. Data brokers are entities "whose principal source of revenue is derived from processing or transferring covered data that the covered entity did not collect directly" from the individual linked to the data.

Rights and Obligations

The APRA would establish rights for individuals from whom covered data is collected and impose obligations on covered entities. Individuals would have the right to access, correct, delete, and export their covered data held by a particular covered entity. When an individual submits a verified request to a covered entity to exercise one of these rights, the covered entity must generally respond within 30 calendar days. Large data holders must generally respond to requests by individuals to exercise their rights within 15 calendar days of receiving the request.

In terms of obligations, the APRA would impose a data minimization requirement on covered entities that would prohibit them from collecting, processing, retaining, or transferring covered data unless it is (1) reasonably necessary and proportionate to provide a specific product or service requested by a consumer or to provide a communication anticipated in the context of the customer relationship; or (2) one of the fifteen expressly permitted purposes listed in the bill (e.g., to conduct market research, investigate and defend against legal claims, or transfer to law enforcement pursuant to lawful process). The APRA would also require covered entities to comply with opt-out and consent requirements. For most covered data, covered entities would need to give individuals an opportunity to opt out of the transfer of their covered data or the use of their data for targeted advertising. For sensitive covered data, however, covered entities would be required to obtain an individual's affirmative, express consent before transferring that data. Covered entities would also be required to get express consent before collecting, processing, or retaining biometric or genetic information.

Covered entities would have to comply with a number of other obligations, including transparency rules, data security standards, and algorithm opt-out requirements. They would also be prohibited from using covered data in a way that discriminates on the basis of a protected class, using "dark patterns" to interfere with individuals' use of their rights, or retaliating against individuals exercising their rights by denying them service or giving them a different level of service (subject to certain exceptions such as for "bona fide loyalty programs").

Large data holders and data brokers would have to comply with additional requirements. For example, large data holders would have to conduct algorithm impact assessments and privacy impact assessments, and their CEOs would have to make annual certifications to the FTC regarding their companies' compliance with the APRA. Data brokers would be required to register with the FTC, which would establish a central data broker registry with a "Do Not Collect" mechanism allowing individuals to opt out of data brokers' collection of their covered data. Data brokers also would be required to establish public-facing websites containing a link to the FTC's data broker registry.

Federal Trade Commission Authority

The APRA would give the FTC authority to enforce violations of the bill. Violations of the APRA, or any regulations issued under it, would constitute violations of rules defining unfair or deceptive acts or practices under the Federal Trade Commission Act, thus giving the FTC the ability to seek civil penalties, injunctions, and other equitable relief for violations. The APRA would create a fund that the FTC could use to disperse civil penalties to persons affected by the penalized conduct.

The APRA would also give the FTC authority to add to and clarify certain provisions of the APRA. While the APRA would not give the FTC broad authority to expound on its provisions through regulations, it would vest the FTC with rulemaking authority in certain instances (e.g., regulations defining categories of sensitive covered data, establishing data security requirements, and creating a process for large data holders to submit algorithmic impact assessments). The APRA also would direct the FTC to issue guidance on how covered entities could comply with certain requirements (e.g., the data minimization provision, data broker disclosure requirements, and algorithm impact assessments). The APRA would further require the FTC to create a process by which covered entities could submit compliance guidelines for approval, and it would require the FTC to establish a pilot program that encourages private-sector use of privacy-enhancing technology.

To carry out its responsibilities, the APRA would direct the FTC to create a new bureau, comparable in size to the existing consumer protection and competition bureaus. The new bureau would need to be staffed and fully operational within one year of the APRA's enactment.

State and Individual Enforcement

The APRA would authorize state attorneys general and state privacy authorities to bring civil actions on behalf of their states' residents. In these actions, state enforcers could ask a federal court to issue an injunction, impose civil penalties, award damages or appropriate equitable relief, and award litigation costs and attorneys' fees.

The APRA also would create a private right of action that would allow individuals to sue for certain violations, for example, disclosure or use of their sensitive, biometric, or genetic information without their consent; violation of their individual rights; and data security violations resulting in a breach of their covered data. In such suits, courts could award aggrieved individuals actual damages, injunctive relief, litigation costs, and attorneys' fees. Before an individual could bring a suit, however, the APRA would require that individual to provide potential defendants with notice and an opportunity to cure the alleged violation (unless the harm qualifies as a "substantial privacy harm"). The APRA also provides that, in certain cases, a plaintiff filing a suit would be entitled to the remedies currently provided under Illinois or California state laws.

In certain circumstances, the APRA allows individuals to pursue claims in federal court, notwithstanding any pre-dispute arbitration agreements. If the claim involves a minor, or if the claim alleges a substantial privacy harm, then the APRA makes any arbitration agreement unenforceable with respect to those claims if the individual harmed elects to proceed in federal court. The APRA clarifies that any disputes over the application of this provision should be resolved by the federal court and not any arbitrator.

Preemption of State Law

The APRA has an express preemption clause providing that no state may "adopt, maintain, enforce, or continue in effect any law, regulation, rule, or requirement covered by the provisions" of the APRA or any regulations promulgated under it. The APRA has numerous exceptions to this preemption clause, however. For instance, the APRA would not preempt, among other things, "consumer protection laws of general applicability," laws addressing the "privacy rights or other protections of employees or employee information," and laws that "protect the privacy of health information, healthcare information, medical information, medical records, HIV status, or HIV testing."

Relation to Existing Federal Privacy Law

The APRA would generally preserve existing federal data privacy and data security laws, such as the Gramm-Leach-Bliley Act, the Health Information Portability and Accountability Act's administrative

simplification provisions and regulations implementing those provisions, the Fair Credit Reporting Act, and the Family Educational Rights and Privacy Act. (For an overview of these federal laws, see CRS Report R45631, *Data Protection Law: An Overview*, by Steve P. Mulligan and Chris D. Linebaugh.) The APRA provides that covered entities that are required to comply with these laws will be "deemed to be in compliance" with the "related provisions" of the APRA. The APRA would, however, displace most privacy requirements under the Communications Act of 1934 and the FCC's implementing regulations. Finally, the APRA specifically preserves the Children's Online Privacy Protection Act of 1998 and "antitrust laws."

Comparison to the ADPPA and Other Privacy Bills

The APRA has many similarities with the ADPPA, containing broadly similar individual rights and covered-entity obligations. There are some differences, however. For example, the APRA would exempt small businesses entirely from its scope, while the ADPPA would have excluded small businesses only from certain requirements. The APRA also does not have some of the protections that the ADPPA would have established for minors under the age of 17, such as its prohibition of targeted advertising and the creation of a Youth Privacy and Marketing Division at the FTC. The APRA, however, contains some obligations not found in the ADPPA, such as the requirement that covered entities give individuals an opportunity to opt out of the use of certain algorithms. While both bills contain a private right of action, the APRA's private right of action would be effective immediately, whereas the ADPPA would have delayed it for two years after the law's enactment. The two bills' preemption provisions have the same basic structure, yet there are several potentially significant differences. For instance, the ADPPA would have expressly preserved several specified state privacy laws, such as Illinois' Biometric Privacy Act and Genetic Information Privacy Act and California's private right of action for victims of data breach. In contrast, under the APRA, these laws would not expressly be preserved, although individuals would be able to obtain the remedies provided by these laws in certain circumstances.

Numerous other comprehensive data privacy bills that further differ from the APRA have been introduced in the 117th and 118th Congresses. For example, rather than specifying detailed user rights and consumer obligations, the Data Care Act of 2023 (S. 744, 118th Cong.) would impose broad duties of care, loyalty, and confidentiality on online service providers. Other bills contain a similar set of individual rights and covered entity obligations as the APRA yet differ on individual enforcement and preemption of state laws. For example, the Online Privacy Act of 2023 (H.R. 2701, 118th Cong.) would provide, and the Consumer Online Privacy Rights Act (COPRA) (S. 3195, 117th Cong.) would have provided, a private right of action without requiring an opportunity to cure or imposing other limitations and would not preempt state laws unless there was a direct conflict with the federal law.

Commentary and Potential Legal Challenges

The draft APRA has garnered bipartisan support, and various interest groups, commentators, and technology companies, such as the Center for Democracy and Technology, the Washington Post's editorial board, and Microsoft, have expressed enthusiasm for the draft bill. Some of these commentators have lauded the bill for compromising on contested issues (namely, whether to provide a private right of action and whether to preempt state laws). At a House Energy & Commerce Committee hearing on April 17, 2024, all of the witnesses agreed that the APRA was the "best chance" for "getting something done" on comprehensive data privacy. At the same time, some of the APRA's supporters have also suggested ways it could be improved. For example, some lawmakers and commentators have said that the APRA's protections for minors should be strengthened, such as by including the ADPPA's ban on targeted advertising to those under the age of 17. Some commentators have also argued that its data broker provisions should be tightened, such as by including a "one-stop-shop for data deletion requests" and

clarifying that data brokers are not exempt from the APRA even if they qualify as consumer reporting agencies under the Fair Credit Reporting Act.

Other stakeholders have been more critical of the draft bill. The California Privacy Protection Agency (CPPA), for example, has faulted the APRA for preempting state privacy laws and has argued that Congress should set a "floor" for privacy rights rather than a "ceiling." The CPPA cited its draft regulations on automated decisionmaking technology (ADMT), which would allow individuals to opt out of companies using their personal information to train ADMT, as an example of an important protection that could be preempted by the APRA. On the other hand, the U.S. Chamber of Commerce has criticized the APRA for taking too narrow of an approach to preemption. The Chamber also took issue with the APRA's private right of action and some of its substantiative requirements, such as its algorithm provisions and its right to opt out of targeted advertising.

Should the APRA be finalized, there may be litigation over its constitutionality and scope. As discussed further in a 2019 CRS report, the U.S. Supreme Court has said that "the creation and dissemination of information are speech within the meaning of the First Amendment." Litigants have challenged laws that restrict the sale or use of data collected from customers and laws that restrict certain targeted advertisements under the First Amendment. It is possible that similar challenges may be raised against some of the APRA's provisions that restrict the dissemination of customer data or the targeting of advertisements. There may also be litigation over the scope of the APRA's preemption provisions. For instance, questions may arise as to whether the APRA preempts state privacy laws that regulate entities not covered by the APRA, such as small businesses. The expansive reach of the APRA's savings clauses, too, may give rise to litigation, as potential challengers of the law might seek to clarify whether various state laws qualify as one of the categories of statutes exempt from preemption.

Author Information

Chris D. Linebaugh
Legislative Attorney

Clay Wild
Legislative Attorney

Peter J. Benson
Legislative Attorney

Jonathan M. Gaffney
Section Research Manager

Matthew D. Trout
Legislative Attorney

Disclaimer