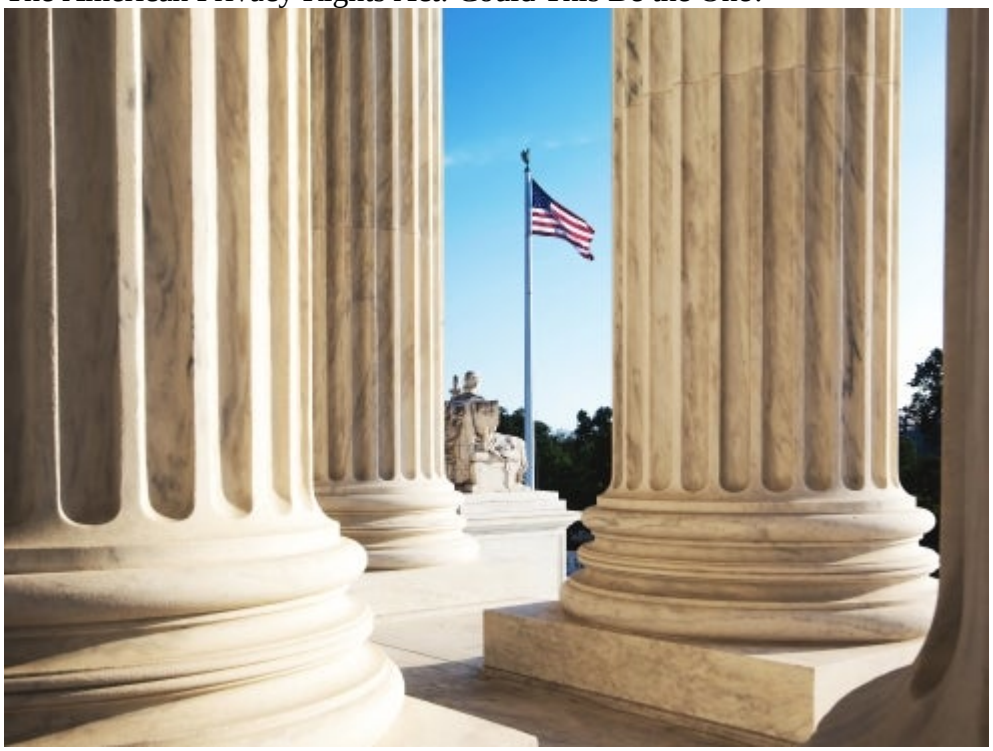
Updates
April 19, 2024
The American Privacy Rights Act: Could This Be the One?



The chair of the U.S. Senate Committee on Commerce, Science, and Transportation, Maria Cantwell (D-WA), and the chair of the U.S. House Committee on Energy and Commerce, Cathy McMorris Rodgers (R-WA), released a discussion draft of the American Privacy Rights Act (APRA) on April 7, 2024.

This announcement of a bipartisan, bicameral bill for a federal comprehensive consumer privacy law was a significant—and unexpected—development in the wake of the American Data Privacy and Protection Act (ADPPA), which never made it to a House floor vote despite bipartisan, bicameral support and considerable attention.

Below is a summary of the APRA's key provisions, which reflect many principles seen in the ADPPA, the wave of omnibus state consumer privacy laws, and Federal Trade Commission (FTC) activity.

Who Is Covered?

The bill would broadly apply to "covered entities"—meaning any business subject to the FTC Act, common carriers under the Communications Act of 1934, and most nonprofits—that alone, or jointly with others, determine the purposes and means of collecting, processing, retaining, or transferring covered data. In a number of provisions, the bill imposes obligations directly on "service providers" as well. The bill has a carve-out for small businesses.

What Is Covered?

APRA's definition of "covered data" largely tracks the definition of personal information under state privacy laws, that is, "any information that identifies or is linked or reasonably linkable, alone or in combination with other information, to an individual or a device." The APRA would exclude de-identified information, employee

information, and publicly available information from covered data.

The bill also provides additional protections for "sensitive covered data," defined to include data considered sensitive under state laws as well as other data deemed sensitive by the FTC or others over the years, such as calendar and address book information, information revealing the content of an individual's video programming viewing, and information of "covered minors" (those under 17 years old).

Data Minimization

Data minimization is at the heart of the APRA. Covered entities (and service providers acting on their behalf) would be prohibited from collecting, processing, retaining, or transferring personal data beyond what is necessary, proportionate, and limited to (1) provision or maintenance of a specific product or service requested by the individual to whom the data pertains; (2) communication that is "reasonably anticipated" in the context of the relationship; or (3) one of 15 expressly permitted purposes (provided the processing is necessary, proportionate, and limited to such purpose). Unlike other laws, the APRA would not permit processing outside the three enumerated categories even with consent.

The APRA's 15 permitted purposes are attracting considerable attention. Along with some of the usual suspects (such as data security and compliance with legal obligations), the bill also lists market research, first-party and contextual advertising, and targeted advertising as permitted purposes. Targeted advertising is curious, as the bill also defines "information revealing an individual's online activities over time and across websites or online services that do not share common branding" as "sensitive." And the use of sensitive information for targeted advertising (as well as first-party and contextual advertising) is expressly excluded from the list of permissible purposes. It is unclear whether this apparent contradiction—allowing targeted advertising with opt-out rights but prohibiting the use of sensitive data for targeted advertising—is intentional.

Processing already-collected data into de-identified data for specific purposes, including product enhancement and development; internal research or analytics to improve a product or service; and public or peer-reviewed scientific, historical, or statistical research would also be permitted.

Processing of sensitive data for two of the otherwise permitted purposes (first-party and contextual advertising and targeted advertising to non-opted-out individuals) would not be permitted, and covered entities would be prohibited from transferring such data without affirmative express consent. Genetic and biometric data would be subject to further limitations.

Transparency

Covered entities would be required to disclose their data practices through detailed privacy policies with requirements similar to those under state laws and additional requirements for "large data holders" (covered entities or service providers that meet certain size thresholds), including short-form notices.

Deletion, Correction, Access, and Portability Rights

As under state laws, the APRA would give individuals the right to access, correct, delete, and port their covered data.

Rights To Opt Out of Data Transfers and Targeted Advertising

As under state laws, covered entities would be required to allow individuals to opt out of "data transfers" (defined to include disclosing or making available covered data by any means for consideration of any kind or for a commercial purpose) and targeted advertising through their own mechanisms and centralized mechanisms such as browser- or device-based global privacy signals developed through FTC rulemaking.

Interference With Rights

The APRA would prohibit the use of "dark patterns" to divert attention from any required notice or to impair an individual's ability to exercise consent. The bill would also prohibit retaliation against individuals for exercising their rights. At the same time, the law would allow covered entities (other than data brokers and high-impact social media companies) to offer "bona fide loyalty programs" subject to highly specific rules.

Data Security

The APRA would require covered entities and service providers to exercise "reasonable data security practices." The bill would also impose a number of specific requirements, such as vulnerability assessments; preventative and corrective actions to mitigate reasonably foreseeable risks; information retention and disposal; training; and incident response.

Governance

Covered entities and service providers would be required to designate one or more qualified employees to serve as "privacy or data security officers." Large data holders would be required to have one employee expressly designated for the privacy officer role, and another for security and to make annual certifications to the FTC.

Data Brokers

The APRA would impose a number of obligations and restrictions on "data brokers," defining that term—more broadly than does, for instance, California—to include not only entities that primarily earn money by selling personal information, but also those that *process* covered data that they don't collect directly from individuals to whom such data relates. For example:

- **FTC registry.** Entities that acted as data brokers with respect to more than 5,000 individuals or devices linkable to an individual in the prior year would be required to register with the FTC, which would maintain a searchable, public registry of data brokers. The registry would offer a "do not collect" opt-out mechanism.
- **Maintain public websites.** Data brokers would be required to maintain a public website that identifies them as a data broker, includes a tool for individuals to exercise their individual controls (e.g., deletion rights and opt-out rights), and includes a link to the FTC registry.
- **Prohibited practices.** Data brokers would be prohibited from using advertising data for stalking, harassment, fraud, identity theft, or unfair or deceptive acts and practices and from misrepresenting their business practices.

Civil Rights and Algorithmic Fairness

The APRA, while not a fulsome artificial intelligence bill, addresses civil rights and algorithmic fairness in the processing of covered data. The bill would broadly prohibit processing covered data in a manner that discriminates or makes unavailable the "equal enjoyment of goods or services" on the basis of protected

classifications. Testing for purposes of reducing discrimination, positive discrimination for diversity purposes, or advertising benefits to underrepresented groups would be exempt.

The APRA would also impose obligations on using "covered algorithms," defined as a "computational process . . . that makes a decision or facilitates human decision-making by using covered data, which includes determining the provision of products or services or ranking, ordering, promoting, recommending, amplifying, or similarly determining the delivery or display of information to an individual," such as the following:

- **Impact assessments.** Large data holders that use covered algorithms in a way that poses "a consequential risk of harm" (e.g., applications relating to minors; making or facilitating ads for healthcare, credit, employment, housing, education, or insurance; determining access to public accommodation; disparate impact based on protected classifications) would have to conduct impact assessments.
- **Algorithm design evaluation.** Covered entities and service providers that knowingly develop a covered algorithm must conduct a predeployment assessment of the algorithm's design, structure, and inputs, including its training data.
- **Notice and opt-out for consequential decisions.** Any entity that uses a covered algorithm to make or facilitate "consequential decisions" (i.e., those affecting access to or equal enjoyment of housing, employment, education, healthcare, insurance, or credit or access to public accommodations) would be required to provide notice to any individual "subject to" use of a covered algorithm and give them an opportunity to opt out of such use.

Enforcement

The APRA would be enforced by federal and state regulators, as well as through a private right of action that is more expansive than in any of the state's comprehensive privacy laws or what had been proposed in the ADPPA:

- **FTC.** The FTC would serve as the federal enforcer and could obtain injunctions, civil penalties, redress/restitution, and damages in federal court. The agency would be required to establish a new bureau dedicated to enforcing the APRA and related matters.
- **States.** States (via their attorneys general, chief consumer protection officer, or an officer or office authorized to enforce privacy or data security laws) could obtain injunctions, civil penalties, damages, and restitution in federal court civil actions.
- **Individuals.** The private right of action has been a sticking point regarding a federal comprehensive privacy bill. The APRA seeks to break through that logjam with a broad private right of action that would apply to many provisions of the law. Relief would include actual damages, injunctions, declaratory relief, and attorneys' fees. In a novel provision specific to private claims regarding biometric or genetic information occurring primarily and substantially in Illinois, the APRA would incorporate statutory damages available under the Illinois Biometric Information Privacy Act and Genetic Information Privacy Act. Similarly, for claims by California residents of unauthorized access to covered data, the bill would incorporate the remedies for data breaches available under California law. There would be a 30-day right to cure prior to lawsuits for injunctive relief, except if the violation resulted in "substantial privacy harm"—defined as any alleged financial harm of at least $10,000; any alleged physical or mental harm to an individual that involves treatment by a healthcare provider; physical injury; highly offensive intrusion into the privacy expectations of a reasonable individual; or discrimination based on specified protected classifications. The APRA would prohibit the enforcement of predispute arbitration agreements for claims alleging a violation involving a minor or substantial privacy harm.

Preemption

Preemption has been one of the most controversial issues. The APRA articulates a purpose of establishing a uniform national privacy and data standard and establishes that state laws that are covered by the APRA are preempted unless they appear in a list of preserved state laws, which includes data breach notice laws, employee privacy laws, and health information laws.

At the federal level, the APRA would expressly preserve the Children's Online Privacy Protection Act. By contrast, the Federal Communications Commission's (FCC) existing obligations on common carriers to protect customer proprietary network information would generally cease to apply, and the FCC would effectively cede privacy-related jurisdiction over common carriers to the FTC. Covered entities and service providers subject to and in compliance with specified federal privacy and data security requirements, such as the Gramm-Leach-Bliley Act and Health Insurance Portability and Accountability Act, would be deemed in compliance with the related privacy provisions of the APRA.

Looking Forward

The House Energy and Commerce Subcommittee on Innovation, Data and Commerce discussed the APRA on April 17, 2024, and consideration by the Senate is likely to soon follow. Many questions remain, such as whether the bill can garner support from critical committee members such as Rep. Frank Pallone (D-N.J.) and Sen. Ted Cruz (R-Tex.). It is unclear at this early stage if the APRA can cross the finish line with all of the competing legislative priorities during a presidential election year. But the release of the discussion draft constitutes significant progress in the march towards national data privacy legislation in the United States and the coming debate around the measure is worthy of close attention.

Authors

Explore more in

Privacy & Security Technology Transactions & Privacy Law Communications

Related insights

Update

HHS Proposal To Strengthen HIPAA Security Rule

Update

California Court of Appeal Casts Doubt on Legality of Municipality’s Voter ID Law