wiley

ALERT

# 10 Things to Know About the APRA – the Latest Federal Privacy Law Effort

April 10, 2024

Over the weekend, lawmakers unveiled the latest push for a federal privacy law – the American Privacy Rights Act (APRA). The bill was circulated as a discussion draft by Sen. Maria Cantwell (D-WA), Chair of the Senate Committee on Commerce, Science and Transportation, and Rep. Cathy McMorris Rodgers (R-WA), Chair of the House Committee on Energy and Commerce. Sen. Cantwell and Rep. McMorris Rodgers represent just "two corners" of the committee leadership that have historically worked on federal privacy legislation; notably missing are the other two corners – Rep. Frank Pallone (D-NJ) and Sen. Ted Cruz (R-TX). Nevertheless, the new APRA is a major development and marks the first bipartisan step forward on federal privacy efforts following last year's American Data Privacy and Protection Act (ADPPA) – which advanced further than any comprehensive privacy law in Congress' history but ultimately never saw a House floor vote.

While it is still early days for the new APRA, the discussion draft is notable in many respects. Below, we ask and answer 10 questions to help provide a high-level summary of the bill and share our initial analysis on how the APRA addresses key issues that have been historical barriers to federal privacy legislation – including preemption and enforcement – and how the bill fits into other policy debates, including AI, children's privacy, and cybersecurity.

***1. What is the relationship between the ADPPA and the APRA?***

The APRA is a new bill that is distinct from the ADPPA. For example, one notable difference between the ADPPA and the APRA is on the issue of kids and teen privacy. The ADPPA, the older bill, had special provisions related to kids and teens under 17, such as a prohibition

## Authors


Kathleen E. Scott
Partner
202.719.7577
kscott@wiley.law

Joan Stewart
Partner
202.719.7438
jstewart@wiley.law

Crystal Tully
Special Counsel
202.719.4348
ctully@wiley.law

Boyd Garriott
Associate
202.719.4487
bgarriott@wiley.law

Kimberly S. Alli
Associate
202.719.4730
kalli@wiley.law


## Practice Areas

Privacy, Cyber & Data Governance
Telecom, Media & Technology

on all targeted advertising to such minors and strict limits on the ability to transfer minors' data to third parties. The ADPPA would also have established a Youth Privacy and Marketing Division at the Federal Trade Commission (FTC) that would have been dedicated to children's privacy regulation. Although the APRA also contains child-specific provisions – such as treating minors' data as "sensitive covered data" – it does not contain many of the ADPPA's minor-specific provisions and would not create a new Division at the FTC.

That said, the new discussion draft is very similar to the ADPPA in many respects. Indeed, the authors of the APRA started from the ADPPA as a base. And the APRA faces similar challenges with respect to state laws as the ADPPA did. The ADPPA was halted last year following its landmark committee vote in part because of concerns about how the federal proposal would interact with state laws, like the California Consumer Privacy Act (CCPA). Early statements from California preview similar challenges for the APRA. For example, in a statement issued by the California Privacy Protection Agency (CPPA) – the new agency in California charged with implementing and enforcing the CCPA – the agency's Executive Director wrote that "Americans shouldn't have to settle for a federal privacy law that limits states' ability to advance strong protections in response to rapid changes in technology and emerging threats in policy."

***2. What types of entities would be covered by the APRA?***

The bill contemplates coverage of a wide swath of the private sector. A **covered entity** would be any entity that (1) determines the purpose and means of collecting, processing, retaining, or transferring covered data *and* (2) is subject to the FTC's authority under the FTC Act, *plus* common carriers subject to Title II of the Communications Act and nonprofits. The bill outlines requirements and parameters for **service providers** to covered entities, as well.

The bill also defines – and establishes special heightened requirements for – **large data holders**, **data brokers**, and **covered high-impact social media companies**.

- "Large data holder" is defined as a covered entity or service provider that in the most recent calendar year (1) had an annual gross revenue of $250,000,000 *and* (2) collected, processed, retained or transferred either the (a) covered data of more than 5,000,000 individuals, 15,000,000 portable connected devices, and 35,000,000 connected devices *or* (b) the sensitive covered data of more than 200,000 individuals, 300,000 portable connected devices, and 700,000 connected devices. The bill would exclude certain data points from counting towards these thresholds – for example, an entity would not be considered a large data holder solely on account of collecting personal mailing addresses, email addresses, or phone numbers.
- "Data broker" is defined as a "covered entity whose principal source of revenue is derived from processing or transferring covered data that the covered entity did not collect directly from the individuals linked or linkable to such covered data."
- "Covered high-impact social media company" is defined as "a covered entity that provides any internet-accessible platform where – (A) such covered entity generates $3,000,000,000 or more in global annual revenue, including the revenue generated by any affiliate of such covered entity; (B) such platform has 300,000,000 or more global monthly active users for not fewer than 3 of the preceding 12

months on the platform of such covered entity; and (C) such platform constitutes an online product or service that is primarily used by individuals to access or share user-generated content."

Of note, the bill does create **various exemptions**, including for:

- Small businesses, defined as an entity whose (i) average annual gross revenues for the preceding three years did not exceed $40,000,000; (ii) that did not collect, process, retain, or transfer the covered data of more than 200,000 individuals for an unauthorized purpose; *and* (iii) that did not transfer covered data to a third party in exchange for revenue or anything of value.
- Governments and entities that are "collecting, processing, retaining, or transferring covered data on behalf of a government entity, to the extent that such entity is acting as a service provider."
- Certain nonprofits that primarily work to (1) prevent, investigate, or deter fraud or (2) train anti-fraud professionals or educate the public about fraud. Of note, this is a limited exception, and these types of entities would still be subject to the APRA's data security and protection obligations.

***3. What types of data are protected?***

The bill defines **covered data** relatively broadly – to include "information that identifies or is linked or reasonably linkable, alone or in combination with other information, to an individual or a device that identifies or is linked or reasonably linkable to 1 or more individuals." Excluded from this definition is: de-identified information, publicly available information, and inferences made from multiple sources of publicly available information that do not meet the definition of sensitive covered data and are not combined with other covered data. Of note, the APRA would also exclude employee data from covered data.

As is the case with state privacy laws, the APRA also defines a special category of **sensitive covered data** – which is subject to heightened requirements. The federal bill's definition of "sensitive covered data" is quite broad including, among other things, information about minors under the age of 17, health data, financial account information, biometric information, precise geolocation information, log-in credentials, and certain web-browsing history. And this definition is subject to further expansion through FTC rulemaking.

***4. What consumer rights would the APRA establish?***

The bill would establish rights that are familiar under many state privacy laws, including the following rights, which are all subject to verifiable requests and all relate to covered data about a specific individual:

- The **right to access** covered data;
- The **right to correct** inaccurate or incomplete covered data;
- The **right to delete** covered data; and
- The **right to export** covered data.

The bill also would establish the **right to opt out** of certain processing – specifically the right to opt out of covered data transfers and the right to opt out of targeted advertising.

While these rights generally track most state privacy laws, there are some significant and noteworthy outliers. For example:

- Under the right to access, the APRA would give individuals the **right to access the specific name of any third party or service provider** to whom covered data has been transferred and the purpose of the transfer. This provision goes beyond any comprehensive state privacy law enacted to date, including Oregon's new law, which itself is an outlier among states in that it contemplates a similar right to access, but only for "third parties" and not for service providers.
- The bill's opt-out rights are also relatively broad compared to state opt-out rights, including an outlier **right to opt out of the transfer of non-sensitive covered data**.

***5. What are the affirmative privacy and security requirements that covered entities would have to meet?***

The bill would impose robust requirements on covered entities (and in many cases service providers too), including:

- **Data minimization requirements:** Covered entities, or service providers acting on behalf of a covered entity, "shall not collect, process, retain, or transfer covered data beyond what is necessary, proportionate and limited" (1) to provide specific goods and services, (2) to send reasonably anticipated communications, or (3) for one of 15 expressly permitted purposes. The bill has additional protections for sensitive covered data (e.g., opt-in consent is required prior to transferring sensitive covered data to a third party) and biometric information and genetic information (e.g., subject to certain exceptions, opt-in consent is required prior to collecting, processing, retaining, or transferring biometric or genetic data).
- **Transparency requirements:** The bill requires covered entities and service providers to make available "in a clear, conspicuous, not misleading, easy-to-read, and readily accessible manner" a privacy policy that accurately details its data collection, processing, retention, and transfer activities. The bill also establishes standards for material changes to privacy policies. Large data holders will have heightened transparency obligations, including being required to (1) retain and publish each previous version of its privacy policy; (2) provide a "short-form" notice; and (3) publish certain metrics regarding consumer rights requests.
- **Executive responsibility requirements:** The bill contemplates two layers of executive responsibility requirements: (1) baseline requirements for all covered entities and service providers, and (2) heightened requirements for large data holders. The heightened requirements for large data holders include certifications to the FTC and required privacy impact assessments, among other requirements.
- **Date security and incident response requirements:** Under the new bill, both covered entities and service providers must "establish, implement, and maintain reasonable data security practices." The law would establish standard reasonable practice requirements, *and* it would prescribe "specific

requirements," such as vulnerability assessments; preventative and corrective actions; information retention and disposal; and training. Additionally, the law would require covered entities and service providers to implement incident response procedures – including detecting, responding to, and recovering from data security breaches.

- **Nondiscrimination requirements:** The bill provides that neither a covered entity nor a service provider may "collect, process, retain, or transfer covered data in a manner that discriminates in or otherwise makes unavailable the equal enjoyment of goods or services on the basis of race, color, religion, national origin, sex, or disability."

***6. Would the federal law preempt other privacy laws?***

As mentioned above, preemption has historically been a politically charged issue that has posed a barrier to adopting a federal privacy law in the past. Given this history, it is no wonder that the preemption provisions in the APRA are complex.

For state privacy laws, at a high level, the latest discussion draft walks a fine line: its general, baseline rule is that it would preempt state laws that are covered by the APRA, but then, it lists a number of state laws that would *not* be preempted, including state breach notification laws, provisions of laws that address employee privacy, and provisions of laws that address health information privacy. The list of exceptions is long and arguably broad, which makes the exercise of determining which laws are preempted and which laws are not a complicated one.

For federal privacy laws, the APRA maps out an equally complex path:

- The bill describes how the APRA would interact with the **FCC's privacy frameworks**, with the authors' Section-by-Section summary explaining that "FCC privacy laws and regulations shall not apply to covered entities with respect to privacy and data security or the collection, processing, retention, or transferring of covered data, PII, customer proprietary network information, personal information, or its equivalent, with the exception of 47 U.S.C. 222(b), (d), and (g); international treaty obligations; and mitigation measures and actions taken pursuant to Executive Order 13913."
- Covered entities or service providers in compliance with other federal privacy requirements – including the **Gramm-Leach-Bliley Act**, the **Health Insurance Portability and Accountability Act**, and the **Fair Credit Reporting Act** – would be deemed "in compliance with the related provisions of" the bill.
- The bill would expressly leave in place the **Children's Online Privacy Protection Act**, providing that the bill would not "relieve or change any obligation" under that statute.

***7. Who would enforce the new APRA?***

The discussion draft contemplates an array of enforcement actors, to include the FTC, state Attorneys General, and private actors:

- **FTC Enforcement:** Of note, the bill would establish a new Bureau in the FTC to implement and enforce the new law, and any violation would be treated as an unfair or deceptive practice under the FTC Act. The bill would also allow the FTC to immediately seek civil penalties for violations of the statute or the agency's regulations – with penalty offsets for any amounts paid in a state or private action against the violator.
- **State AG Enforcement:** States would be able to seek a range of relief for violations of the new law, including injunctive relief, civil penalties, restitution, and other appropriate relief.
- **Private Right of Action:** The APRA would establish what appears to be a broad and complicated private right of action for consumers who allege violations of the law. While the law's default remedy is actual damages, injunctive relief, and attorney's fees, in some instances (for example, with respect to claims about biometric and genetic information involving conduct in Illinois and certain data breaches impacting California residents), the consumer may seek statutory damages. The bill contemplates an opportunity for the covered entity to cure prior to lawsuits in some – but not all – circumstances. The bill would also prohibit arbitration agreements as to claims alleging violations of the privacy law that involve a minor or that result in a substantial privacy harm.

***8. How does the bill impact the FTC's Privacy Rulemaking process?***

The APRA would launch a range of **FTC rulemaking** activity, including proceedings to establish rules to expand the definition of sensitive covered data, rules to establish a centralized opt-out mechanism for consumers' opt-out rights, and rules for covered algorithm impact assessments.

Interestingly, the law – if adopted – would also terminate the FTC's current privacy rulemaking regarding Commercial Surveillance and Data Security.

***9. Would the APRA regulate AI?***

Not surprisingly, the APRA would establish special rules for **covered algorithms**, defined as "a computational process, including one derived from machine learning, statistics, or other data processing or artificial intelligence techniques, 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." For example, it would:

- Require a covered entity or service provider that knowingly develops a covered algorithm to engage in a design evaluation;
- Require large data holders that use covered algorithms in a manner that poses a consequential risk of harm to conduct risk impact assessments; and
- Require an entity that uses a covered algorithm to make or facilitate a consequential decision to provide notice and opt-out rights.

Note that several of these requirements apply where covered algorithms make or facilitate consequential decisions – a concept that is defined broadly by the bill to be "a determination or an offer, including through advertisement, that uses covered data and relates to – (1) an individual's or a class of individuals' access to or equal enjoyment of housing, employment, education enrollment or opportunity, healthcare, insurance, or credit opportunities; or (2) access to, or restrictions on the use of, any place of public accommodation."

***10. What are the next steps for the APRA?***

While the discussion draft was authored by the chairs of the two major committees of jurisdiction, building support from other key legislators and stakeholders will be critical for the bill to advance. For example, Rep. Frank Pallone, the House Energy and Commerce Committee's Ranking Member, called the bill "very strong" but indicated he wanted to strengthen protections for children online. Sen. Ted Cruz, the Senate Commerce Committee's Ranking Member, was more critical in his statement, noting that he "cannot support any data privacy bill that empowers trial lawyers, strengthens Big Tech by imposing crushing new regulatory costs on upstart competitors or gives unprecedented power to the FTC …" Taking a step back from the specific statements, what is clear is that there is still work to be done on the bill, and that work will take time.

Process-wise, Chair McMorris Rodgers expressed her desire to move the legislation through regular order. To this end, the House Energy and Commerce Committee scheduled a legislative hearing for April 17 to discuss the APRA. The hearing will also hear testimony on the Kids Online Safety Act (KOSA) and the Children's Online Privacy Protection Act (COPPA) – legislation that could be incorporated into the APRA. However, with limited legislative days remaining in a presidential election year, Congress will have to move quickly if the bill has a chance to be enacted.

***

Wiley's Privacy, Cyber & Data Governance team has helped entities of all sizes from various sectors proactively address risks and address compliance with new privacy laws. Please reach out to any of the authors with questions.