Privacy Alert
April 2024

A Federal Privacy Law? What You Need to Know About the Draft American Privacy Rights Act

With 15 states passing their own consumer privacy laws, federal lawmakers unveiled a new privacy discussion draft, the American Privacy Rights Act (APRA). This federal proposal was brokered by Washington Sen. Maria Cantwell (the Democratic chair of the Senate Committee on Commerce, Science and Transportation) and Washington Rep. Cathy McMorris Rodgers (the Republican leading the House Committee on Energy and Commerce).

The fact that Senate Democrats and House Republicans were able to reach any kind of agreement is noteworthy. Over the years, the parties have constantly and consistently disagreed on a handful of key issues, federal preemption and a private right of action being chief among them. In the spirit of compromise, APRA provides for federal preemption (meaning, the bill would supersede similar state laws); however, APRA would not preempt state laws based on consumer protection, civil rights, employee privacy, student privacy, data breach notification, public records and medical records (among others). APRA would still allow much of the privacy-related litigation we're seeing, however, as laws regarding electronic surveillance and wiretapping, cyberstalking and blackmail, and unsolicited email and phone laws would remain intact. APRA proposes a somewhat complicated private right of action, where consumers could seek actual damages for certain substantial privacy harms. And with respect to litigation, more broadly, APRA would prohibit or otherwise invalidate arbitration provisions for privacy violations of a minor (a child under the age of 17), as well as claims alleging a substantial privacy harm.

Who does APRA apply to?

APRA applies to a "covered entity" that determines the purposes or means of collecting, processing, retaining or transferring covered data and is otherwise subject to the Federal Trade Commission (FTC) Act (which is most businesses, with some exceptions concerning banks, insurance companies, and air carriers). The bill would apply to certain nonprofits and common carriers — two entities not usually regulated by the FTC. Small businesses, governments and entities working on behalf of governments are generally excluded.

The bill defines a "small business" as an entity whose average annual gross revenue for the past three years did not exceed $40 million and did not collect or process covered data of more than 200,000 individuals. "Covered data" is defined as "information that identifies or is linked or reasonably linkable, alone or in combination with other information, to an individual or a device." Covered data excludes de-identified data, employee information, publicly available information and some inferences made only from independent sources of publicly a vailable information.

Attorney Advertising

"Large data holders" are subject to additional requirements such as retaining and publishing their privacy policies from the past 10 years and also providing a short-form notice of their policies. A "large data holder" is an entity that has $250 million or more in annual revenue, or collects covered data of more than 5 million individuals or the sensitive data of more than 200,000 individuals.

What does APRA generally require?

- **Data minimization** – covered entities (and service providers) are prohibited from collecting, retaining or processing data beyond what is necessary, proportionate and limited to providing the product or service requested or to communicate with consumers. Covered data can only be used for a "permitted purpose," which includes things like complying with legal obligations; conducting market research; transferring data to a third party as part of a merger, bankruptcy or similar transaction; or preventing or detecting fraud.
- **Transparency** – covered entities are required to make privacy policies and data privacy and security policies publicly available. And when making a material change to a privacy policy, the covered entity must provide advance notice and a way to opt out of the processing or transfer for previously collected data. Large data holders must also make their privacy policies publicly available for the past 10 years, and include a short-form notice.
- **Consumer requests** – similar to state privacy laws, consumers have the right to request access, correction or deletion of their covered data. Consumers are also entitled to know the name of any third party or service provider to which their covered data was transferred, the category of sources from which the covered data was collected, and the purpose of such transfer.
- **Targeted advertising opt-out** – consumers have the right to opt out of targeted advertising, which is defined as presenting an online ad to an individual or device identified by a unique persistent identifier, based on known or predicted preferences or interests associated with the individual or device identified by a unique identifier. Similar to other state laws, "targeted advertising" does not include (1) advertising or marketing to a consumer in response to their specific request for information or feedback; (2) first-party advertising based on the consumer's visit to or use of a website or online service that offers a product or service related to the subject of the ad; (3) contextual advertising; or (4) processing data for ad measurement or reporting (including media performance, reach or frequency). Although the bill includes a targeted advertising opt-out, data required for targeted advertising (like data relating to "online activities over time and across third-party websites") would be considered "sensitive data," for which the covered entity would need affirmative express consent. The broad definition of sensitive data and the targeted advertising opt-out would seem to severely limit the types of advertising entities are able to engage in without consent.
- **Data security** – covered entities must establish data security practices that are appropriate to the entity's size, the nature and scope of the entity's data practices, the volume and sensitivity of the data the covered entity collects or processes, and "state of the art" administrative, technical and physical safeguards for collecting covered data.
- **Executive responsibility** – covered entities must designate at least one employee to serve as a data security officer. Large data holders must designate a data security officer and a data privacy officer. Along with the chief executive officer, the data security officer and data privacy officer of a large data holder must file annual certifications with the FTC regarding the covered entity's internal controls.

What about sensitive data?

Covered entities must obtain affirmative express consent before collecting biometric or genetic information, or transferring "sensitive covered data." The bill takes an expansive view of what's considered sensitive covered data. Sensitive covered data includes data from a covered minor, health information, biometric and genetic information, financial account and payment data, precise geolocation, and account credentials. But it also includes additional data such as private communications, information revealing sexual behavior, private photos and recordings, video programming viewing information, and, notably, online activities over time and across third-party websites or over time on any website or online service

operated by a covered high-impact social media site. The bill would give the FTC the ability to make rules to further define sensitive covered data.

What about AI?

Somewhat similar to previous legislation that we've seen, and in line with the Biden Administration's broader priorities, APRA has a section dedicated to civil rights and algorithms. "Covered algorithms" are defined as computational processes or other data processing or artificial intelligence that make a decision or facilitate human decision-making by using covered data. Covered entities that design a covered algorithm must conduct an evaluation prior to deploying the algorithm and must provide the evaluation to the FTC and make it publicly available. Large data holders that use a covered algorithm in a way that poses a consequential risk of harm are required to conduct an impact assessment. That assessment must be provided to the FTC and also made publicly available. The FTC has the power to issue rules on the submission of those impact assessments and whether (or to what extent) low- or minimal-risk algorithms could be exempt from this requirement.

Where a covered entity uses an algorithm to make consequential decisions (like those related to housing, employment, education, health care, insurance, credit or access to places of public accommodation), the consumer must be provided with the ability to opt out.

What about children's data?

Under APRA, data from a minor (a child under the age of 17) would be considered sensitive covered data. APRA also specifically states that nothing in the law would relieve or change any covered entity's Children's Online Privacy Protection Act (COPPA) obligations. However, unlike other comprehensive privacy laws, APRA is fairly quiet on child-privacy provisions. Given the other children's privacy proposals floating around Congress, like the Kids Online Safety Act and COPPA 2.0, many believe that those bills may be paired up with APRA as a "privacy package" or that one of those bills could be added into APRA.

What happens next?

The APRA discussion draft gives new momentum to a comprehensive federal privacy bill, but there are still some hurdles ahead before it could become law. We have already heard from some legislators that changes are needed. Rep. Frank Pallone (ranking member of the House Committee on Energy and Commerce) supports the bill but suggested that there are some key areas where it could be strengthened — children's privacy being one of them. Sen. Ted Cruz (ranking member of the Senate Committee on Commerce, Science and Transportation) is reportedly critical of APRA, citing the private right of action and FTC rulemakings as his main concern.

Regardless, both the House and Senate committees appear eager to dig in and are moving quickly. APRA is already scheduled for a hearing in the House Committee on Energy and Commerce on April 17 (where the committee will also hear a host of other privacy-related bills), and we expect the Senate Commerce Committee to announce a hearing in the next few weeks.

Related Professionals

Robyn Mohr . . . . . rmohr@loeb.com
Chanda Marlowe . . . . . cmarlowe@loeb.com
Teodoro "Teddy" Shelby . . . . . tshelby@loeb.com