Articles + Publications | April 12, 2024

Comprehensive Data Privacy Legislation Unveiled in Congress

WRITTEN BY

Kim Phan | Robyn W. Lin

On April 7, House Energy & Commerce Committee Chair Cathy McMorris Rodgers (R-WA) and Senate Commerce Committee Chair Maria Cantwell (D-WA) announced a bipartisan, bicameral draft of comprehensive data privacy legislation, the American Privacy Rights Act (APRA). The APRA represents a significant compromise and, according to Rodgers and Cantwell, "strikes a meaningful balance on issues that are critical to moving comprehensive data privacy legislation through Congress," such as preemption of state laws and a consumer private right of action.

Applicability

Covered entities subject to the APRA include companies under the jurisdiction of the Federal Trade Commission (FTC). Additionally, the APRA explicitly includes nonprofit organizations. It defines other covered entities subject to heightened requirements, including data brokers and large data holders. The APRA also outlines obligations for service providers to covered entities.

The APRA's protections apply to individual data, as well as device data if reasonably linkable to an individual. It defines a subcategory of covered data to capture sensitive covered data, including biometrics, precise geolocation, financial account numbers, login credentials, device information (*e.g.*, calendar, contacts, photos, phone logs, etc.), online activities, and more. Importantly, covered data would not include employee information.

The APRA provides a small business exemption for any company that satisfies the following criteria: (1) did not exceed annual gross revenue of $40 million for the three preceding calendar years; (2) did not process data of more than 200,000 individuals; and (3) did not sell covered data to third parties.

Obligations

Data minimization: Covered entities must comply with data minimization principles by not processing covered data beyond what is necessary, proportionate, and limited to providing a specific product or service or as reasonably anticipated within the context of the relationship with an individual.

Privacy policy: Covered entities must also make publicly available a privacy policy, which details the identity and contact information of the covered entity; categories of covered data that are collected, processed, and retained; the processing purpose for each such category of covered data; each category of service provider or third party to

which the covered entity transfers covered data; the name of each data broker to which covered data is transferred; and the purposes for any such data transfers; the length of time covered data is retained; how individuals can exercise their data rights; a general description of data security practices; the effective date; and whether any covered data is made accessible to any foreign adversary of the nation. The privacy policy must be available in each language that the covered entity provides a product or service or otherwise carries out its activities. The privacy policy must also be accessible to individuals with disabilities.

The APRA would establish a notice and opt-out requirement for any material changes to privacy policies. If an individual opts out, a covered entity would be required to discontinue any processing or transfers of any previously collected covered data.

Large data holders would have additional transparency obligations and be required to publish copies of any prior versions of privacy policies over the past 10 years. Large data holders would also be required to develop a "short-form" version of its privacy policies, which must not exceed 500 words.

Data rights: Covered entities must provide individuals with rights to access, correction, deletion, and portability of covered data. Individuals would be permitted to make up to three verified requests per year at no charge, although a covered entity could charge a reasonable fee for any additional requests during a 12-month period. Covered entities would have 30 calendar days to respond to such requests, while large data holders would be required to respond within 15 calendar days. Covered entities would be permitted only one extension of time to prepare responses. While the APRA provides for some limited exceptions from responding to such requests, a covered entity would still be required to provide adequate explanation of any decision to decline a request and would still be required to partially comply to the extent not subject to any asserted exception. Large data holders would be required to publish metrics about the number of verified requests and their responses.

Covered entities would be required to provide a mechanism for individuals to opt out of the transfer of covered data, as well as targeted advertising.

Covered entities would be prohibited from using "dark patterns" or otherwise interfering with the exercise of an individual's data rights. This includes a prohibition against any discrimination, denial or service, or other retaliation against an individual.

Data security: Covered entities would be required to maintain reasonable data security practices, including at a minimum, assessing vulnerabilities, taking preventive and corrective action to mitigate reasonably foreseeable internal or external risks, disposing of covered data when no longer necessary, training employees, and implementing incident response procedures.

Accountability: Covered entities would be required to designate a privacy or data security officer to implement the requirements of the APRA and facilitate ongoing compliance. Large data holders would be required to designate a privacy officer and a data security officer. Large data holders would also be required to certify to the FTC on an annual basis as to its internal controls to comply with the APRA and its internal reporting structure for certifying officers, including the chief executive officer. Large data holders would also be required to conduct annual privacy impact assessments.

Contract requirements: Written agreements entered into between a covered entity and a service provider would be required to contain specific provisions setting forth instructions for collecting, processing, retaining, or transferring data; the nature and purpose of the collection, processing, retention, or transfer; the type of data subject to collection, processing, retention, or transfer; the duration of the processing or retention; and the rights and obligations of both parties. Service providers generally would not be permitted to combine covered data which the service provider receives from or on behalf of a covered entity with another entity.

Data brokers: Covered entities whose principal source of revenue is derived from processing or transferring covered data that was not collected directly from the individuals would be considered data brokers. Such data brokers would be required to register with the FTC, which will be made publicly available on a searchable registry. The registry would include a mechanism for individuals to submit a request to all registered data brokers not to collect covered data about the individual without affirmative express consent.

Algorithmic decisions: Covered entities that make consequential decisions using covered algorithms would be required to provide notice to the individual about how the covered algorithm makes or facilitates consequential decisions and the range of potential outcomes. Covered entities would also be required to provide an opportunity for such individual to opt-out of the use of such covered algorithm. Covered entities and service providers that develop a covered algorithm would be required to evaluate the design, structure, and inputs of the covered algorithm, including any training data used to develop the covered algorithm, to reduce the risk of the potential harms. Large data holders would be required to conduct annual impact assessments of consequential risks of harm from the use of covered algorithms. Any such impact evaluations or assessments would be required to be submitted to the FTC.

Enforcement

The FTC would be required to establish a new bureau to exercise the FTC's authority, including enforcing violations of the APRA as an unfair or deceptive act or practice.

The APRA may also be enforced by the states. States would be required to notify the FTC in writing prior to initiating a civil action to enforce the APRA, which will allow the FTC the opportunity to intervene in such action.

The APRA also grants individuals a private right of action to enforce the APRA. Individuals would be able to pursue actual damages, injunctive relief, declaratory relief, and attorney's fees as part of any such civil action. However, prior to seeking actual damages, the individual must provide the covered entity with 30 days' written notice. For actions seeking injunctive relief, following such notice from an individual, covered entities would have a 30-day period to cure the alleged violations, unless the individual is alleging a substantial privacy harm.

The APRA would make any pre-dispute arbitration agreement invalid and unenforceable for individuals under the age of 18 years and for alleged violations resulting in substantial privacy harm.

Preemption

The APRA was designed by the bill sponsors to eliminate "the patchwork of state laws by setting one national privacy standard, stronger than any state." It would purportedly, "establish a uniform national data privacy and

data security standard in the United States to prevent administrative costs and burdens placed on interstate commerce" and expressly preempt state laws.

Several exemptions from such state preemption are included in the APRA, such as state privacy laws that address employee information, sector specific obligations, electronic surveillance and wiretapping, telephone solicitations, etc.

The preemption of state laws has already attracted pushback from California Privacy Protection Agency Executive Director Ashkan Soltani. Soltani released a statement in response to the draft saying 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." He also calls on the Congress to set a federal floor on privacy, and not a ceiling.

Federal Exemptions

A covered entity or service provider that complies with specified federal laws and regulations would be deemed to be in compliance with the APRA, including:

- Gramm-Leach-Bliley Act
- Health Insurance Portability and Accountability Act
- Fair Credit Reporting Act
- Family Educational Rights and Privacy Act

Rulemaking

The FTC is empowered to issue APRA regulations in several areas, including the development of a centralized consent and opt-out mechanism; guidance for data brokers; identifying any additional exceptions under the APRA; etc.

The APRA would terminate the FTC's current proposed rulemaking on commercial surveillance and data security.

Next Steps

The House Energy & Commerce Committee has already scheduled a hearing for April 17 to discuss the draft legislation as well as other privacy bills.

If enacted, covered entities would have only 180 days before the APRA takes effect.

RELATED INDUSTRIES + PRACTICES

- Privacy + Cyber