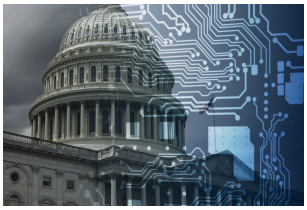

Decoding the American Privacy Rights Act of 2024: What Your Business Needs to Know about the Proposed Privacy Framework

May 01, 2024

Categories:

Publications
Technology Blog

Authors:

Ashley J. Earle
Lauren E. Cole
Jean Paul Yugo Nagashima

**This article was published by Security Info Watch on May 17, 2024.*

The American Privacy Rights Act of 2024 ("APRA"), a bill recently introduced by House Energy & Commerce Committee Chair Cathy McMorris Rodgers and Senate Commerce Committee Chair Maria Cantwell, aims to address data privacy concerns in the United States. It would regulate consumer data privacy and security, data minimization, safeguards for generative AI systems, transparency of data processing, data processing by large data holders, and greater control for individuals over their personal information. Importantly, the APRA would preempt—meaning it would override—the existing state privacy laws (though there are quite a few exceptions). Preemption has been a contentious issue for the passage of comprehensive federal privacy legislation.

The APRA would apply to companies subject to the Federal Trade Commission (FTC) Act, and even goes a step farther to reach nonprofit entities (collectively, "covered entities"). Some small businesses (under $40 million in revenue and processing covered data of less than 200,000 individuals) would be exempt, unless they generate revenue from sharing covered data with third parties. The APRA would cover all individuals and would treat information about minors (defined as individuals under the age of 17) as sensitive covered data.

What Does the APRA Propose?

1. Protection of Covered Data

The APRA would protect the "covered data" of individuals by an entity that determines the purpose and means of collecting, processing, retaining or transferring the data. Covered data includes

information that identifies or is linked or reasonably linkable to an individual or a device that is linked or reasonably linkable to one or more individuals. This broad definition does not include de-identified data, employee information, publicly available information, inferences made exclusively from multiple independent sources of publicly available information (with certain conditions), and information in the collection of a library, archive, or museum.

In addition, APRA requires further safeguards for the collection and use of sensitive covered data. Sensitive covered data includes the same categories in state privacy laws, such as information revealing race, ethnicity, national origin, or sex, government-issued identifiers (e.g., a social security number or driver's license number), information that describes an individual's past, present, and future health conditions and treatments, genetic information, financial account information, biometric information, precise geolocation information. The APRA considers private communications, account or device log-in credentials, information revealing sexual behavior, information regarding minors, images and recordings intended for private use or depicting the naked or undergarment-clad private area of an individual, an individual's viewing log video programming, information revealing an individual's online activities across websites, and other information the FTC determines to be sensitive covered data.

2. Consumer Data Rights

The APRA requires covered entities to provide consumers with rights about their covered data and how it may be processed. These rights include:

- **Right to access** their covered data;
- **Right to correction** of their covered data;
- **Right to deletion** of their covered data, and
- **Right to portability** of their covered data.

Covered entities must have flexibility and agility in their data storage practices allowing for deletion or correction and to provide portability. For example, if an individual requests a copy of all of

their covered data collected, the covered data can be exported in an accessible manner to be shared with the individual. These rights apply even if that data is going to be shared with a competitor or made public (except for derived data if it would result in the release of trade secrets or other proprietary or confidential data).

3. Opt-Out Mechanisms

The APRA allows consumers to opt out of covered data processing and covered data use, including opting out of targeted advertising, algorithmic decision making and covered data transfers. The opt-out process should be straightforward and transparent. The APRA further directs the FTC to establish requirements and technical specifications for a centralized mechanism for opt-outs within two years of the APRA's enactment. For covered entities using algorithmic decision making, the APRA requires a clear and conspicuous notice to individuals that provides meaningful information on how the algorithm makes or facilitates a consequential decision—i.e., decisions that affect an individual's housing, employment, education enrollment, healthcare, insurance or credit opportunities.

4. Data Minimization and Purpose

The APRA emphasizes that covered data should be restricted to specific, expected uses. This mirrors the language used in General Data Protection Regulation of the European Union regarding data minimization and requiring a clear purpose for data collection. Covered entities, as well as their service providers, should closely examine their data collection practices and steer clear of the "collect everything we can and sort it out later" mentality—all information collected and retained should have a clear, explicit, specified purpose.

5. Impact Assessments for Large Data Holders

Privacy impact assessments (PIAs) evaluate the impact of proposed data processing on privacy. Covered entities with more than $250 million in revenue and that collect large amounts of

covered data or *sensitive* covered data ("large data holders") must conduct these PIAs to consider the potential risks and benefits of data collection. Covered algorithms— a computational process that makes a decision or facilitates human decision making by using covered data—are also subject to impact assessments, and large data holders are required to detail the steps taken to mitigate the risk of harm to the following: minors, housing, education, employment, health care, insurance, credit opportunities, public accommodations based on protected characteristics, or disparate impacts based on such characteristics or on political party affiliation. Additionally, these PIAs and covered algorithm impact assessments should be transparent and clearly articulated, with recommendations to manage, minimize, or eliminate privacy-related impacts to a community.

6. Data Privacy and Security Officer

Covered entities and service providers are required to have one qualified employee to serve as a privacy or data security officer. Large data holders would be required to have two officers—a privacy *and* a data security officer. The data security officer must be a designated, qualified employee that oversees the organization's data protection efforts and ensures compliance with the APRA's requirements regarding consumer privacy rights, data minimization, and cybersecurity measures. Large data holders that trigger this requirement would be required to annually certify to the FTC their internal controls for APRA compliance and the reporting structure for the data security officer and other certifying officers, including the company's CEO.

7. Private Cause of Action

The APRA would permit individuals to sue with a private right of action for violations of the APRA. The legislation also would not allow for mandatory arbitration clauses if the case involved minors, a substantial privacy harm ($10,000), or specific physical or mental harms. An individual may seek actual damages, injunctive relief, declaratory relief, and reasonable attorneys' fees and litigation costs. This provision could lead to class action lawsuits and is very

controversial. In addition to individuals, FTC or state attorney generals may enforce the APRA.

8. Preemption

Non-sectoral state privacy laws are preempted by the APRA. That means laws that address specific subsections of privacy rights, including employment, education, breach notifications, banking, health, and other narrow laws, are not preempted, but privacy laws that generally address all categories of personal data and all rights to the data as provided in the APRA will be superseded by the APRA. This can help to greatly simplify the U.S. data privacy framework, but not all state regulators are happy with this idea based on the APRA having broader or narrower protections in comparison to their own laws.

Next Steps in the Process

Overall, while this proposed legislation does take a bipartisan approach and seems to have generated substantial support politically from both sides of the aisle, the APRA contains a few controversial points (e.g., preemption, private cause of action, whether the FTC has such broad enforcement power, the 17-and-under age limit for minors) that have some questioning whether it will be passed into law. The bill's current "effective date" is 180 days after enactment, but only time will tell if this law will quickly pass the scrutiny of the House of Representatives and the Senate.

Now that the bill has been proposed, it will undergo committee review where it will likely face proposed amendments and changes before floor consideration. Once approved in committee, the APRA would move to consideration by the full House of Representatives and Senate, with voting by both chambers (a simple majority vote required for passage) and, finally, if passed by both, would need to be signed into law by the president. However, these processes can, at times, happen very quickly, and companies should start preparing now in case the bill is signed into law and the short turnaround for the effective date remains—provided that six months is not a long window to comply with these drastic changes to privacy practices. Covered entities would be wise to make sure

their policies and procedures are in line with the APRA requirements as soon as possible.

For more information and guidance, or to update your current policies and practices to comply with the APRA, please contact the authors of this article or any member of Frost Brown Todd's Data Security and Privacy practice group.

FBT Gibbons