DAVIS GILBERT

Privacy, Technology + Data Security

U.S. House Unveils the Latest Attempt at a U.S. Privacy Law: The American Privacy Rights Act

The Bottom Line

- If passed, the APRA would largely supersede the intricate patchwork of state privacy laws, and set sweeping new standards for privacy regulation in the U.S.
- While the law would simplify privacy compliance by reducing the number of laws to follow, it would also make compliance more challenging in some respects.
- The APRA is still a long way from passage, and its survival is far from certain. Additional hearings and feedback from key stakeholders are expected in the coming months.

The United States is among the minority of large economies in the world without a comprehensive national privacy law. In the absence of such a law, numerous states are filling the void with a complex assortment of often inconsistent privacy laws.

However, unexpected legislative developments in the U.S. House of Representatives will potentially resolve the challenges raised by the current patchwork of conflicting state laws. On April 7, 2024, House members announced a draft bill for the American Privacy Rights Act (APRA). The bill still has many hurdles to overcome and may ultimately share the same fate as prior failed attempts at a federal privacy law. But if enacted, the APRA would upend the U.S. privacy landscape.

Preemption of State Laws by APRA

The APRA's intent is to "establish a uniform national data privacy and data security standard in the United States." As such, it would expressly preempt state laws that cover the same requirements as the APRA. This means that comprehensive privacy laws, such as the California Consumer Privacy Act (CCPA), Colorado Privacy Act, Connecticut Data Privacy Act (CTDPA) and others, would be preempted, in whole or in part, in exchange for the federal law. State data broker laws in Vermont, California, Texas and Oregon would also likely be neutralized, since the APRA sets

rules and requirements for data brokers, including the establishment of a national data broker registry.

There are, however, some notable exemptions to the APRA's preemption standard that would preserve certain portions of states' frameworks. Most important is the law's exception for "provisions of laws that protect the privacy of health information, healthcare information, medical information, medical records, HIV status, or HIV testing." This would allow the stringent requirements of the Washington My Health My Data Act and Nevada S.B. 370 to survive APRA's passage. Recent amendments to the CTDPA that extend the law's scope to "consumer health data" and "consumer health data controllers" would, in theory, also largely remain intact. Additionally, the APRA exempts "provisions of laws that address the privacy rights or other protections of employees or employee information," which means that much of the CCPA could be salvaged to the extent that it applies to employee data.

APRA's Threshold Requirements

The APRA applies to "covered entities," which means any entity that determines the purposes of processing and is subject to the Federal Trade Commission (FTC) Act, including common carriers and certain nonprofits. Entities are exempt from the APRA, though, if they meet the criteria of a "small business," expressly defined as an entity:

- with less than $40 million in annual revenue,
- that annually processes the covered data of 200,000 individuals or less (with exceptions relating to payment processing) and
- that did not transfer covered data to a third party in exchange for revenue or anything of value.

The combination of the $40 million revenue and 200,000 individual thresholds would, in theory, exempt many businesses from the law's scope. However, the additional criteria regarding transferring covered data to third parties "in exchange for revenue or anything of value" likely means that any online service that conducts targeted advertising would potentially fall within the law's scope, no matter its size.

APRA's Legal Obligations

The APRA imposes obligations on covered entities with respect to "covered data," defined as "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 one or more individuals."

These obligations include, but are not limited to:

- **Data minimization**: Processing of covered data is generally prohibited unless it is necessary, proportionate and limited to specific products or services or communications expected by the individual or falls under one of the law's enumerated purposes.
- **Transparency**: Covered entities are required to publish a privacy policy, and material changes to such a policy requires advance notice to individuals and the means to opt out of further processing of any previously collected data that would be subject to those changes.
- **Consumer rights**: Covered entities are required to offer individuals the rights of access, deletion and correction with respect to their data. Individuals also have the right to opt out of data transfers generally, as well as the right to opt out of targeted advertising.
- **Service providers and third parties**: The APRA appears to have adopted the CCPA's business/service provider/third-party approach in lieu of the controller/processor model followed by most comprehensive privacy laws. Covered entities must exercise due diligence in selecting service providers and in deciding whether to transfer covered data to a third party.
- **Data brokers**: The FTC is empowered to develop a national data broker registry, and data brokers processing the data of 5,000 or more individuals must register annually. Data brokers are also required to have a public website that includes tools for individuals to exercise their privacy rights.

Additional obligations apply to covered entities that are "large data holders," which are covered entities that have $250 million or more in annual revenue and process large amounts of covered data of individuals and devices (as statutorily defined). Large data holders are required to:

- publicly post all privacy versions from the past 10 years,
- publish annual transparency reports,
- provide CEO-signed certifications of compliance to the FTC,
- appoint data privacy and data security officers,
- conduct biennial audits and privacy impact assessments and
- submit impact-risk assessments to the FTC for certain algorithmic decision-making activities.

Sensitive Data

The APRA sets heightened rules for processing "sensitive covered data." While the law's definition of "sensitive" shares many similarities with the CCPA, CTDPA and other laws, such as government-issued identification numbers, race/ethnicity and health data, there are some surprising departures from the established norm at the state level. Sensitive-covered data under the APRA includes:

- Precise geolocation information, which is defined not only to include accuracy up to 1,850 feet or less, but also information that reveals "street-level location information of an individual or device;"
- Calendar information, address book information, phone or text logs, photos, audio recordings or videos intended for private use;
- A photograph, film, video recording or other similar medium that shows the naked or undergarment-clad private area of an individual;
- Certain transfers of information revealing the extent or content of any individual's access, viewing or other use of video programming with respect to an individual's vision or hearing impairment;
- Certain information that reveals the video content requested or selected by an individual and
- Information revealing an individual's online activities over time and across websites or online services that do not share common branding or over time on any website or online service operated by a covered high-impact social media company.

This last element may be the most significant for the advertising industry since it would turn common-place retargeting on the internet into the processing of sensitive data. As a result, cookie banners may become much more prevalent as companies constantly seek consent from consumers to use their browsing data in this manner. While not required by law in the United States, cookie banners are already advisable due to the significant rise in class action lawsuits alleging violations of decades-old privacy laws (such as the Video Privacy Protection Act and California Invasion of Privacy Act) that require consent in certain cases.

The APRA's consent obligations for sensitive data are less stringent than most of the state comprehensive privacy laws on the books. Although opt-in consent is required for any collection of biometric or genetic data, all other types of sensitive-covered data only require opt-in consent for transfers of such data to a third party.

APRA Enforcement

The APRA would be enforced by the FTC, which would be empowered to create a new bureau to carry out its authority under the law. Violations would be treated as a *per se* unfair or deceptive practice under Section 5 of the FTC Act. The APRA is also enforceable by state attorneys general, who must notify the FTC prior to initiating a civil action in federal court.

Critically, the APRA would provide individuals with a private right of action for violations concerning:

- opt-in consents to collect or transfer sensitive data,
- making material changes to a privacy policy without providing notice and the ability to opt out,
- an individual's data access, deletion, correction or opt-out rights, including retaliation against an individual for exercising such rights,
- data breaches caused by failure to adopt reasonable security practices,
- failure to conduct reasonable due diligence over service providers and third parties that receive covered data,
- discrimination based on protected characteristics and
- certain obligations relating to algorithmic decision-making.

For More Information

Please contact the attorneys listed below or the Davis+Gilbert attorney with whom you have regular contact.

Richard Eisert

Partner
212 468 4863
reisert@dglaw.com

Gary Kibel

Partner
212 468 4918
gkibel@dglaw.com

Zachary Klein

Associate
212 237 1495
zklein@dglaw.com