Insight

Where Congress Stands on the American Privacy Rights Act

JEFFREY WESTLING, AYEN MIHIDUKULASURIYA | JULY 29, 2024

Executive Summary

- In April, a bipartisan, bicameral group of lawmakers introduced the American Privacy Rights Act (APRA) to establish comprehensive national standards for data privacy and protection.
- APRA aims to enhance consumer control over personal data, enforce data minimization, ensure transparency and consent, mandate robust data security measures, hold companies accountable for algorithmic decisions, protect children's privacy, prohibit discriminatory data practices, and designate the Federal Trade Commission as the primary enforcement authority.
- Despite bipartisan support, APRA may fail to pass if lawmakers cannot find an appropriate compromise on longstanding disagreements about preemption of state laws, the inclusion of a private right of action, and the inclusion of other privacy legislation for minors.

Introduction

In April of 2024, a bipartisan, bicameral group of lawmakers introduced the American Privacy Rights Act (APRA) to establish a comprehensive national framework for data privacy in the United States. This legislation aims to unify data privacy standards across the country, addressing concerns about personal data misuse and breaches.

APRA introduces stringent requirements for data collection, usage, and security, ensuring that individuals have greater control over their personal information. Despite bipartisan support, however, the bill could become the latest in a long line of comprehensive privacy frameworks that ultimately fail to pass both chambers. Of note, disagreements on the extent to which national privacy law should preempt state laws and whether individuals should have the right to sue for a violation of the law have prevented similar legislation from passing. APRA attempts to balance the countervailing considerations. Legislators have also pushed to pass APRA in conjunction with additional child privacy legislation, further adding complexity to the discussion.

This primer discusses what APRA would do and how it attempts to balance the long-standing disagreements on the key issues of state-law preemption and a private right of action.

Provisions of APRA

APRA would create comprehensive requirements for how companies, including nonprofits and common carriers, handle personal data, defined as information that identifies or is reasonably linkable to an individual. Specifically, the bill mandates that most companies limit the collection, processing, and transfer of personal data to what is reasonably necessary to provide a requested product or service or under other specified circumstances. It generally prohibits the transfer of personal data without the individual's affirmative express consent. The bill would also grant robust consumer data protections, granting individuals the right to access,

correct, and delete their personal data. Companies must offer an opt-out mechanism for targeted advertising.

APRA primarily designates the Federal Trade Commission (FTC) to issue regulations to enforce these security requirements but also grants authority to state attorneys general and state consumer protection officers. Notably, starting two years after the bill takes effect, individuals may bring civil actions for violations, subject to certain notification requirements.

Finally, the bill preempts some state laws covered by its provisions, with exceptions for certain categories of state laws and specific laws in Illinois and California.

Considerations for Congress

Preemption of State Laws

Under APRA, comprehensive state privacy laws, such as the California Consumer Privacy Act, would largely be preempted. This means that federal law would supersede state laws, creating a single set of rules for businesses to follow. Proponents argue that this would reduce the administrative burden and compliance costs associated with navigating varying state regulations, particularly for businesses operating in multiple states. By providing a uniform standard, APRA would simplify compliance efforts and create a more predictable regulatory environment for businesses??.

Not all state privacy laws would be preempted, however. Proponents of state-level privacy laws to supplement a federal standard have argued that state laws can often provide stronger protections than federal laws. As a result, through negotiations, the preemption provisions of the law have largely been watered down, with many state laws explicitly being excluded from the preemption language, such as the private right of action provisions for data breaches included in California law. Further, broad categories of laws such as consumer protection laws of general applicability, civil rights, and contract law are explicitly not preempted. Finding the appropriate preemption balance will be critical for garnering strong support.

Private Right of Action

Another critical issue in the debate over the American Privacy Rights Act of 2024 is the inclusion of a private right of action, which allows individuals to sue for violations of their privacy rights. This provision is a significant point of contention between privacy advocates and businesses.

Privacy advocates argue that a private right of action is essential for ensuring robust enforcement of privacy rights. Without the ability for individuals to directly sue companies for privacy violations, businesses may not take compliance seriously, they claim. This provision enables consumers to seek redress for breaches of their privacy, acting as a powerful deterrent against non-compliance and fostering greater corporate responsibility regarding data protection.

Conversely, businesses and some lawmakers oppose the inclusion of a private right of action, fearing it would lead to a surge in litigation. They argue that this provision could open the floodgates to lawsuits, many of which might be frivolous or opportunistic, placing an undue burden on businesses, especially smaller companies that may lack the resources to defend against numerous lawsuits. Previous versions of the bill allowed the FTC to intervene before a private action could proceed, but newer versions of the bill have curtailed these provisions, drawing significant scrutiny from Republican leadership in the House.

Kids' Privacy

Finally, the House has attempted to attach updates to the Children's Online Privacy Protection Act (COPPA) with APRA, which could complicate passage.

COPPA, enacted in 1998, gives parents control over the information collected from their children online. It requires websites and online services aimed at children under 13 to obtain verifiable parental consent before collecting, using, or disclosing personal information from children. The law also mandates that these websites and services post clear privacy policies, maintain the confidentiality, security, and integrity of the information collected from children, and provide parents with access to their child's data.

APRA specifically incorporates updates to COPPA, reinforcing and expanding many of its provisions. For example, APRA would extend COPPA's requirements to a broader range of digital services and platforms, and reforms knowledge requirements to put more liability on platforms when the platform should infer that they are collecting information from a minor. These provisions could garner some additional support among privacy advocates, they could also drive opposition from critics who worry the bill places undue burdens on businesses.

Conclusion

With stringent requirements for data collection, usage, and security, APRA would give individuals greater control over their personal information. Passage is far from clear, however, and longstanding disagreements over the shape and scope of a federal privacy framework have yet to be fully resolved.