Cybersecurity Law Report cslawreport.com

May 22, 2024

Federal Legislation

Proposed Broad Private Right of Action Under a New Federal Privacy Law Could Be a Plaintiff's Paradise

By Jeewon Kim Serrato, Shruti Bhutani Arora and Christine Mastromonaco, *Pillsbury*

On April 7, 2024, the Senate Commerce Committee Chair Maria Cantwell (D-WA) and House Energy and Commerce Committee Chair Cathy McMorris Rodgers (R-WA) jointly released the text of the American Privacy Rights Act (APRA), a draft piece of legislation to establish a federal data privacy standard. Updated text of the APRA was released on May 21, 2024, just 36 hours before the House Energy and Commerce Subcommittee on Innovation, Data and Commerce hearing to mark up the initial draft. On May 23, the the subcommittee unanimously passed the updated draft and it was sent to the full committee. In the updated text, the private right of action section remains unchanged. As drafted at the time of this writing, the APRA marks a monumental departure from the limited private enforcement available under current state privacy law.

The proposed comprehensive federal privacy law, ntitles individuals to bring civil suits against entities that violate their rights under the law. As drafted, the APRA marks a monumental departure from the limited private enforcement available under current state privacy law.

This article discusses the details of the APRA's private right of action, the remedies available to individuals and the preemptive effect of the APRA.

See our two-part series on private actions under the California Privacy Rights Act: "Key Issues and Defense Strategies" (Oct. 18, 2023), and "Settlement Considerations and Mitigating Risk" (Oct. 25, 2023).

Private Right of Action

The APRA gives enforcement authority to (a) the FTC, the AG of a state, the chief consumer protection officer of a state, or an officer or office of the state authorized to enforce privacy or data security laws applicable to the covered entity or service provider; and (b) the individuals.

Potential Claims

Under Section 19 of the APRA, individuals may file civil actions for violation in the following circumstances:

Failure to Obtain Consent

Plaintiffs can allege that a company did not obtain affirmative express consent before processing their sensitive data. Whether consent was obtained in accordance with a legal requirement is likely to raise an issue of material fact.

Similarly, whether a business transferred sensitive covered data without affirmative consent is likely to be an issue for summary judgment. In this same vein, whether a business adequately offered individuals a way to withdraw their consent is likely to be a factual dispute of Section 3(b).

Failure to Protect Biometric Data

Plaintiffs can bring an action against an entity that fails to provide additional protections for Biometric Information[1] and Genetic Information[2]. Specifically, they may allege that such entities failed to obtain affirmative express consent before transferring such information to third parties. Other violations may involve failure to provide individuals with a legally compliant method to withdraw affirmative express consent in accordance with Section 3(c).

Failure to Clearly Communicate Privacy Policy and Any Material Changes

Plaintiffs can sue businesses for alleged failures to provide a clear, conspicuous, not misleading, easy-to-read, readily accessible privacy policy that provides a detailed and accurate representation of the covered entity or service provider's data collection, processing, retention and transfer activities, in accordance with Section 4(a).

Allegations of this nature will likely involve disputes of material facts. For example, litigating the issue as to whether a business's notice was misleading will necessitate a factual inquiry as to whether there was a material departure between the business's practices and representations, as well as whether a reasonable individual would have been misled.

Plaintiffs also can bring an action for failure to notify the affected individuals about any material changes in the privacy policy and the means to opt out of such processing or transfer of data, in accordance with Section 4(e). Whether change is "material" will probably involve mixed questions of law and fact.

Failure to Provide Access, Correction or Deletion

Plaintiffs may sue covered entities that fail to provide individuals with the right to access, correct, delete and port their data, in accordance with Section 5.

Failure to Deliver Opt-Out Rights

Plaintiffs may seek redress against entities that fail to provide them with a clear and conspicuous means to opt out of the transfers of covered data and the ability to make that decision through an opt-out mechanism. Likewise, covered entities that engage in targeted advertising and fail to provide a clear and conspicuous means for individuals to opt out of such targeted advertising through an opt-out mechanism may also be subject to civil actions in accordance with Section 6(a).

Under Section 6(b)(2), plaintiffs may bring an action alleging that an entity failed to abide by requirements related to the opt-out mechanism. Questions of when and whether the individual submitted a request, whether the opt-out mechanism was valid, whether the individual opted back in, and when the business allegedly failed to abide by an opt-out signal may raise questions of fact.

Use of Dark Patterns

Plaintiffs can sue entities for a violation of the prohibition against using dark patterns to impair user decision making or obtain consent, in accordance with Section 7. Whether a device "divert(s) an individual's attention from any notice required under [the APRA]" or "impair(s) an individual's ability to exercise" their rights may require factual determinations.

Retaliation

Plaintiffs can bring a civil action against a business for retaliating against them for exercising any right.

Abuse of Loyalty Program

Plaintiffs can sue entities that fail to obtain affirmative express consent for an individual's participation in a bona fide loyalty program as well as the transfer of their data in connection with a bona fide loyalty program. Likewise, plaintiffs may seek redress in the event the entity fails to provide individuals with means to withdraw from a bona fide loyalty program, in accordance with Section 8.

Whether consent was obtained as required under a legal requirement and/or whether the method to withdraw consent was legally sufficient may raise an issue of material fact.

Insufficient Data Security Practices

Plaintiffs can bring a lawsuit for violations of the requirement that a covered entity or service establish a reasonable data security practice to protect the confidentiality of covered data and protect such data against authorized access, in accordance with Section 9(a).

Whether an entity's data security practices were reasonable will likely be a question of fact involving a determination as to the specific circumstances of any alleged breach and case-specific factors such as the nature of the business and the adequacy of security measures implemented.

Failure to Use Due Diligence With Third Parties

Entities may face lawsuits where plaintiffs allege the entity failed to use reasonable due diligence in selecting a service provider, in accordance with Section 11(d). Whether a business exercised reasonable due diligence may involve determinations of fact.

Failure by Data Broker to Respond to a "Do Not Collect" Request

Plaintiffs can bring a lawsuit for a violation of the requirement that data brokers comply with a "Do Not Collect" request from an individual using an approved mechanism. Section 12(c)(4). A data broker, upon receiving the Do Not Collect request, is required to stop collecting covered data related to the individual without the affirmative express consent of such individual, except if the data broker is acting as a service provider.

Discrimination

Individuals can bring a claim alleging a violation of the prohibition against collecting, processing, retaining or transferring covered data in a manner that discriminates on the basis of race, color, religion, national origin, sex or disability, in accordance with Section 13(a). Such claims may involve factual disputes about the nature of the discrimination alleged.

Use of Algorithm

Plaintiffs can bring a claim against entities that use a covered algorithm to make or facilitate a consequential decision but fail to provide notice to individuals and an opportunity for individuals to opt out of such use, in accordance with Section 14.

Available Remedies

Under Section 19(a)(2) of the APRA, individuals could seek actual damages, injunctive relief – including an order that the entity retrieve any covered data transferred in violation of the APRA – declaratory relief, and reasonable attorney's fees and litigation costs.

See "A Roadmap to the Final Regulations Under the CPRA" (Mar. 15, 2023).

Cure Period

Except in instances where an individual seeks injunctive relief for a violation of the APRA that resulted in substantial privacy harm, individuals must provide an entity with written notice of violation prior to bringing an action. Entities are then given a 30-day period to cure any violations. This cure provision may allow entities to manage their exposure by promptly rectifying violations.

Under the APRA, "substantial privacy harm" would mean: (1) any alleged financial harm of not less than $10,000; or (2) any alleged physical or mental harm to an individual that involves (a) treatment by a licensed, credentialed or otherwise bona fide healthcare provider, hospital, community health center, clinic, hospice, or residential or outpatient facility for medical, mental health or addiction care; or (b) physical injury, highly offensive intrusion into the privacy expectations of a reasonable individual under the circumstances, or discrimination on the basis of race, color, religion, national origin, sex or disability.

See "To 'Cure' or Not to 'Cure,' That Is the Question" (Jun. 9, 2021).

Mandatory Arbitration

The APRA also has provisions that put limits on mandatory arbitration. Any terms of service mandating arbitration would be deemed unenforceable for claims alleging a violation involving minors or claims resulting in substantial privacy harm.

Broader Than State Laws

The APRA significantly expands the scope of the private right of action that currently exists under operative provisions in U.S. state laws.

While the APRA allows individuals to initiate a civil action against an entity that violates their rights, the California Consumer Privacy Act, as amended by the California Privacy Rights Act (CCPA) only permits private actions for breaches of data security requirements. The CCPA provides a private right of action to an individual whose "nonencrypted and nonredacted personal information" is "subject to an unauthorized access and exfiltration, theft, or disclosure as a result of the business's violation of the duty to implement and maintain reasonable security procedures."

While Washington and Florida comprehensive privacy law bills each had a provision for a private right of action, these laws were never passed. Washington's My Health My Data Act includes a fairly broad private right of action for consumers, just like the Illinois Biometric Information Privacy Act (BIPA). BIPA litigation trends could be an indicator for how the private right of action may play out under the APRA, as currently written.

In early May 2024, the Vermont Legislature passed House Bill 121 for an act relating to enhancing consumer privacy. The bill, which still requires the Governor's signature to become law, is set to be one of the strongest in the nation, with an expansive private right of action available to consumers against data brokers and "large data holders" – *i.e.*, those which process the personal data of more than 100,000 state residents – for violations of the prohibition on processing sensitive personal data without consent. This provision, however, may cause the bill to be rejected as Vermont Governor Phil Scott is reportedly concerned that it would subject the state's businesses to frivolous claims.

See "BIPA Decisions Expand Potential Liability: What's Next in Illinois and Other States?" (Mar. 8, 2023); and "Progress? Recent Rulings Are One Step Forward, Two Steps Back for BIPA Defendants" (Feb. 7, 2024).

Preemptive Effect of APRA

The APRA states it is intended to "establish a uniform national data privacy and data security standard." Therefore, it would preempt state law covered by the APRA.

Preservation of Existing Laws and Allowance for New Laws

The APRA enumerates extensive exceptions that would preserve provisions of state laws related to:

- employee privacy;
- student privacy;
- banking records, financial records, tax records, social security numbers, credit cards, identity theft, credit reporting and investigations, credit repair, credit clinics or check-cashing services;
- electronic surveillance, wiretapping or telephone monitoring;
- unsolicited email messages, telephone solicitation or caller ID;
- data breach notifications; and
- health privacy.

In addition to preserving the above state law provisions, it appears that – if the processing of information is not governed "solely and exclusively" by the federal regulations enumerated in it – the APRA also allows for the states to enact new privacy and security laws in the same categories.

The APRA would also preserve several rights to statutory damages under state law. For example, in civil actions brought for violations related to biometric and genetic information in Illinois, the act would preserve relief set forth in BIPA and the Genetic Information Privacy Act. The APRA would also preserve statutory damages for security breaches under the CCPA, as mentioned above.

See our two-part series on Washington's aggressive health privacy law of 2023: "Right to Sue and Onerous Consent Obligations" (May 3, 2023), and "Ten Compliance Priorities" (May 10, 2023).

Application of Federal Privacy and Security Laws

The APRA does not have entity-level exemptions for covered entities or service providers that are subject to existing federal privacy laws, such as for covered entities and their business associates subject to the Health Insurance Portability and Accountability Act (HIPAA) and financial institutions subject to the Gramm-Leach-Bliley Act (GLBA). Rather, the APRA offers a data usage level exemption, which means that such entities would not have to comply with the APRA if the information was used "solely and exclusively" with respect to the privacy and security laws and regulations enumerated in the APRA, such as HIPAA, GLBA the Fair Credit Reporting Act, and the Family Educational Rights and Privacy Act.

See our two-part series examining the California Privacy Protection Act close-up: "Review of Amendments and How to Prepare for Compliance" (Oct. 2, 2019), and "Examining the GLBA Carve-Out and How Financial Institutions Can Evaluate Applicability" (Oct. 9, 2019).

Opposition and Next Steps

The APRA's broad private right of action and limited preemption are two of the central issues that are certainly under debate as Congress continues to mark up the draft proposals.

While a comprehensive U.S. federal privacy law would serve both individuals and industry, Congress should consider how such a wide departure from existing private right of action provisions in state laws may result in businesses' limited resources being tied up on frivolous litigation, used to extract costly settlements.

As currently drafted, there may also be litigation over the scope of the APRA's preemption provisions. There could be questions as to whether the APRA preempts state privacy laws that regulate entities not covered by the APRA. The APRA's savings clause is also expansive and may give rise to potential challenges, as clarification may be needed on whether various state laws qualify as one of the categories of statutes exempt from preemption.

On April 16, 2024, the California Privacy Protection Agency (CPPA) sent a letter to the Chairs of the House Energy & Commerce Committee and the Innovation, Data, and Commerce Subcommittee "outlining the ways in which the [APRA] discussion draft seeks to weaken privacy protections for Californians."

On May 8, 2024, AGs of 14 states along with the AG of California, Rob Bonta, urged Congress "to adopt legislation that sets a federal floor, not a ceiling, for critical privacy rights and respects the important work already undertaken by states to provide strong privacy protections" for the residents of these states.

Time may be running out to pass meaningful federal privacy legislation ahead of the 2024 presidential election. Ongoing efforts are needed to address the current concerns and provide strong privacy protections as a new national standard that would replace the current patchwork of laws.

Jeewon Serrato is a partner in San Francisco and global head of Pillsbury's consumer protection practice. She counsels clients in the areas of consumer privacy, cybersecurity, data optimization and data science. Serrato also advises clients on compliance with the FTC Act and various state consumer protection, unfair competition and deceptive practices acts, and represented Sephora in the first CCPA settlement with the California AG. She formerly worked on Capitol Hill and served as head privacy executive for a global data broker and a publicly traded financial services company with $3.5 trillion in assets.

Shruti Bhutani Arora is a partner in Pillsbury's consumer protection practice in San Francisco. She counsels clients on implementation of programs, policies and procedures for the purposes of complying with state and federal privacy and cybersecurity laws and helps with the drafting and negotiating of complex technology contracts.

Christine Mastromonaco is a senior associate in Pillsbury's consumer protection practice in San Francisco. She counsels clients in a variety of industries, including tech, retail, healthcare and financial services on data optimization strategies, consumer privacy and regulatory defense matters. Mastromonaco has previously represented financial services and fintech clients in state and federal courts in a wide array of commercial and class action matters.

[1] "Biometric Information" means "any covered data that is specific to an individual and is generated from the measurement or processing of the individual's unique biological, physical, or physiological characteristics that is linked or reasonably linkable to the individual, including – (i) fingerprints; (ii) voice prints; (iii) iris or retina imagery scans; (iv) facial or hand mapping, geometry, templates; or (v) gait." It does not include "(i) digital or physical photograph; (ii) an audio or video recording; or (iii) metadata associated with a digital or physical photograph or an audio or video recording that cannot be used to identify an individual."

[2] "Genetic Information" means "any covered data, regardless of its format, that concerns an identified or identifiable individual's genetic characteristics, including – (A) raw sequence data that results from the sequencing of the complete, or a portion of the extracted deoxyribonucleic acid (DNA) of an individual; or (B) genotypic and phenotypic information that results from analyzing raw sequence data described in subparagraph (A)."