Published on *The National Law Review* https://natlawreview.com

Proposed Bill Would Substantially Rewrite the California Consumer Privacy Act of 2018

Article By:

James R. Kalyvas

Steven M. Millendorf

Michael R. Overly

Eileen R. Ridley

Proposed Changes At-A-Glance

- Renames the California Consumer Privacy Act of 2018 as the Privacy for All Act of 2019
- Requires an affirmative opt-in consent by consumers for sharing of personal information
- Businesses can only delay, but not refuse, a consumer's right to delete data for so long as reasonably necessary for one of the exceptions to no longer apply
- Increases transparency obligations regarding data sharing activities, including specifics of personal information shared and the entities with whom personal information is shared
- Increases diligence requirements for service providers and narrows the safe harbor for service provider violations
- Makes fundamental changes to a consumer's private right of action and other statutory damages, increasing potential exposure and liability to businesses
- Incorporates broader regulatory enforcement actions
- Delays the effective date until January 1, 2021

On April 4, 2019, California Assembly Member Wicks proposed sweeping changes to bill AB 1760, effectively repealing the California Consumer Privacy Act of 2018 (CCPA) and replacing it with the Privacy for All Act of 2019 (PAA). The proposed rewrite would increase a business's compliance obligations as well as its potential exposure to civil and regulatory liability, shifting California even closer to the requirements of GDPR. If passed, the PAA will go into effect on January 1, 2021, giving businesses one additional year to implement the new requirements.

Requirements of the PAA

- **Affirmative Opt-In Consent.** While the CCPA only required opt-out consent for the selling of personal information, the PAA would require businesses to provide California consumers with an affirmative opt-in consent to share that consumer's personal data. Furthermore, sharing under the PAA includes all forms of selling, renting, releasing, disclosing, disseminating, making available, transferring, or otherwise communicating and, unlike the CCPA, no monetary or valuable consideration is required. Like other affirmative opt-in consent requirements, businesses will not be able to pre-check the opt-in consent — consumers must perform an affirmative act for the consent to be valid. In addition, the collection of data from children under 13 years of age still requires opt-in consent from a parent or guardian.

- **Exceptions to Right to Delete.** The PAA would also significantly restrict a business's ability to refuse a California consumer's request to have his or her personal information deleted. Under the PAA, a business will only be able to delay its compliance with a consumer's request for deletion only for so long as reasonably necessary until one of the enumerated exclusions no longer applies. Under the PAA, a business would be required to automatically comply with the request once none of the exceptions apply without a further request from the consumer. Additionally, the business will be required to delete all of the consumer's data regardless of the source, not just data collected from that consumer by the business.

- **Increased Disclosure Obligations.** Under the CCPA, businesses were only required to disclose the categories of personal information shared and the categories of third parties with whom the personal information was shared. Under the PAA, businesses would be required to also disclose the specific pieces of personal information disclosed as well as the specific third parties to whom the personal information was disclosed. Businesses will also be required to contractually prohibit downstream recipients from re-identification of consumer information, and must make reasonable efforts to ensure service providers comply with the PAA.

- **Expanded Definition of Personal Information.** The CCPA already had a broad definition of personal information, which included information that identifies, relates to, describes, is capable of being associated with, or could reasonably be linked, directly or indirectly, with a particular California consumer or household. The PAA would expand the definition of personal information to include information that could be linked with a device, including, for example, network MAC addresses and device serial numbers. However, while the CCPA excluded from the definition of personal information publicly available information made available from federal, state, and local government when the information was used for a purpose compatible with the purpose for which the information was maintained, under the PAA all information (other than biometric information) lawfully made available from federal, state, or local governments would be excluded.

- **Increased Liability for Violations by Service Providers.** The PAA would significantly

expand exposure to liability of businesses for their service providers' violations of the PAA. Under the CCPA, a business was not liable for the violations of its service providers if, at the time of the disclosure of personal information, the business had no knowledge of or reason to believe the service provider intended to violate the CCPA. Under the PAA, a business would not be liable for its service providers' violations of the PAA only if the business has made reasonable efforts to ensure that the service provider will comply with the PAA and the business has no actual knowledge of or reason to believe that the service provider violated the PAA. Essentially, the PPA creates a duty on businesses to audit their vendors and confirm their compliance with PPA.

- **Increased Private Rights of Action.** Under the current version of CCPA, a California consumer could bring a private right of action only for data breaches resulting from failures to reasonably protect personal information and only after the consumer provided the business notice and an opportunity to cure. Under the PAA, California consumers would be able to bring a private right of action for any violation of the PAA without providing the business pre-suit notice or an opportunity to cure. The PAA also explicitly permits California consumers to recover reasonable attorney's fees in addition to other statutory damages of no less than $100 and up to $750 or any other relief the court deems proper.

- **Increased Regulatory Enforcement.** The PAA would expand the scope of potential regulatory actions from actions brought by the Attorney General's office with a 30-day cure period to actions brought by any district attorney, city attorney, or county counsel with no cure period. In addition to injunctive relief, fines remain at up to $2,500 for each unintentional violation and up to $7,500 for each intentional violation.

The CCPA and Proposed PAA Compared

CCPA	PAA
Opt-out consent for selling personal information.	Opt-in consent for sharing personal information.
The term "selling" is limited to selling, renting, releasing, disclosing, disseminating, making available, transferring, or otherwise communicating for monetary or other valuable consideration.	The term "sharing" includes selling, renting, releasing, disclosing, disseminating, making available, transferring, or otherwise communicating, with no monetary or valuable consideration required.
Businesses can refuse to delete personal information if one of the exceptions apply.	Businesses may only delay deleting personal information until none of the exceptions apply.
Must disclose the categories of personal information sold and the categories of third parties to whom the personal information is sold.	Must also disclose the specific personal information shared and the specific third parties with whom the personal information is shared.
Definition of personal information means information that identifies, relates to, describes, is capable of being associated with, or could reasonably be linked, directly or indirectly, with a particular consumer or household.	Definition of personal information now includes information that identifies, relates to, describes, is capable of being associated with, or could reasonably be linked, directly or indirectly, with a particular consumer, household, or device.
Businesses are not liable for violations by their service providers if, at the time of disclosure, they have no actual knowledge of or reason to believe	Businesses are not liable for violations of their service providers if (a) at the time of disclosure, they have no actual knowledge of or reason to

that the service provider intends to commit such a violation.	believe that the service provider committed those violations and (b) the business makes reasonable efforts to ensure compliance by the service provider.
California consumers can bring a private right of action only for data breaches resulting from failures to reasonably protect personal data and only after a notice and opportunity to cure. Statutory damages of $100-$750 and any other relief that the court deems proper.	California consumers can bring a private right of action for any breach of the PAA, with no notice or opportunity to cure. California consumers can now recover reasonable attorney's fees in addition to the statutory damages of $100-$750 and any other relief that the court deems proper.
Attorney General can bring regulatory actions with 30 days' notice and opportunity to cure. Can receive injunctive relief and fines between $2,500-$7,500 per violation.	Attorney General as well as any district attorney, city attorney, or any county counsel can bring an action with no cure period. Can receive injunctive relief and fines between $2,500-$7,500 per violation.

Applicability to Businesses

The PAA would continue to apply to for-profit entities that do business in California that also determine the purposes and means of the processing of California consumers' personal information, and that either: (a) have annual gross revenues in excess of $25,000,000 (anywhere); (b) annually process the personal information of 50,000 or more California residents, households, or devices; or (c) derive at least half of their gross revenue from the sharing of personal information of California consumers.

The PAA excludes the same businesses as are excluded from the CCPA, such as: Medical Information governed by California's Confidentiality of Medical Information Act or protected health information subject to the privacy, security, and breach notification rules under the Health Insurance Portability and Accountability Act; information collected as part of a clinical trial subject to human subject protections under the Common Rule, the International Conference on Harmonisation's "Guideline for Good Clinical Practice," or the U.S. Food and Drug Administration; the sale of personal information to or from a consumer reporting agency used to generate consumer reports and in compliance with the Fair Credit Reporting Act; information processed, sold, or shared pursuant to the Gramm-Leach-Bliley Act; and information collected, processed, sold, or shared pursuant to the Drivers' Privacy Protection Act. It also would not apply when a business believes in good faith that an emergency exists that requires sharing of personal information, or when information is shared with the National Center for Missing and Exploited Children in connection with a report.

Impact on Businesses

Although the PAA, if passed, will not go into effect until 2021, it will take time for impacted businesses to comply with all of its provisions. Businesses subject to the PAA should consider the following actions in preparation for the PAA implementation:

- Conduct a data mapping of the personal information collected by the business to understand the scope of personal information collected and how it is obtained, used, and shared with third parties.

- Review internal policies and procedures to be able to appropriately respond to consumer requests for access to, deletion from, or information related to the sale or disclosure of their

personal information.

- Begin the planning and implementation of technological improvements to their information systems that may be necessary to process consumer requests and consumers' rights to opt-in to the sharing of personal information. Businesses may wish to consider the use of technology features that enable easy moves between opt-in and opt-out consents in the event this requirement is not present in the final law.

- Review and update privacy policies to comply with the disclosure requirements of the PAA when it becomes necessary to do so.

- Begin preparing training materials and planning for training all personnel who are responsible for handling consumer personal information inquiries.

- Update contracts with third parties and/or service providers to whom consumer personal information is conveyed to ensure that the contracts explicitly limit the use of personal information to providing the services contemplated, permit the business to audit the vendor's operations for compliance with PPA and contractual terms, and require the vendor to assist with consumer requests.

- Review vendor due diligence procedures (including audits) to verify that service providers are able to comply with the PAA.

- Consider including defense, indemnification, and insurance provisions in favor of the business in all contracts with vendors given access to consumer information.

- Consider using third-party audits to ensure compliance with the PAA and conducting those audits through legal counsel to support the position that the results are covered by the attorney-client privilege.

Although AB 1760 has only now been formally introduced, Assembly Member Wicks has been discussing the PAA for a few weeks. In February, she stated that "Consumers should have the right to find out what data companies have collected on them, how that information is being used, and to stop their personal information from being shared and sold." While the fate of the PAA remains in question, we expect that we will see several concepts from the PAA become law. There is already significant lobbying taking place on behalf of the PAA, including by the ACLU of California, Common Sense Kids Action, Consumer Reports, Electronic Frontier Foundation, and the Privacy Rights Clearinghouse. In addition, often considered a more liberal state, California is seeing a backlash resulting from the rushed, closed-door process of drafting the CCPA — which some have called "pay-for-privacy" and holding the right to opt out hostage — opening the door for an increasing groundswell for a "fair deal for all."

On the other hand, the PAA does not incorporate other proposed changes to the CCPA that have received significant support, making it likely that we will see the PAA amended again. For example, AB 25 proposed to remove employee personal data from the scope of the CCPA, which is not reflected in the PAA as it is currently drafted. It is also worth noting that many businesses in California are calling for the CCPA enforcement date to be pushed back, as even those business that are taking an aggressive, proactive response to complying with the CCPA fear they will not be compliant by January 1, 2020. Many businesses are also concerned about the look-back period

created by the CCPA, as almost no company can say it was compliant with the CCPA as of January 1, 2019. Given all of the above and more, we are seeing efforts to push back the effective date of the CCPA to 2021, like the PAA is proposing. Nevertheless, it remains unclear whether California Governor Newsom will sign the bill into law, as the CCPA was signed into law by his predecessor, former Governor Brown.

National Law Review, Volume IX, Number 100