

California Adopts Sweeping Consumer Privacy Law



IN SHORT

The Situation: Unanimously passed by the California state legislature, the California Consumer Privacy Act of 2018 introduces the nation's most wide-ranging consumer data privacy laws.

The Result: New consumer protections include an expanded definition of "personal information," disclosure requirements for companies collecting consumer information, opt-in and opt-out rights, and various other related measures.

Looking Ahead: The law becomes effective in January 2020.

The State of California has adopted the most comprehensive consumer data privacy laws in the United States similar to other foreign jurisdictions. On June 28, 2018, Governor Jerry Brown signed the California Consumer Privacy Act of 2018 ("AB-375") into law. Unanimously passed by the California state legislature, the statute will impose significant changes on how businesses collect, store, sell, and otherwise process consumer personal information, significantly changing the data privacy legal landscape for large businesses in the United States. When the law comes into effect in January 2020, consumers will have expanded control over their personal information, and businesses will have additional obligations related to notice, disclosure, and response to consumer requests.

Expanded Definition of "Personal Information"

AB-375 introduces a broad definition of "personal information," including "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." This includes not only the personal information regulated by existing privacy law (Social Security numbers, driver's licenses, and financial account numbers), but also IP addresses, employment-related information, purchase history, personal characteristics, and internet search history. Additionally, the definition includes "[i]nferences drawn from any of the [personal information] to create a profile about a consumer."

Disclosure Requirements

Businesses will be obligated to provide a consumer, at or before the point of collection, with notice "as to the categories of personal information to be collected and the purposes for which the categories of personal information shall be used." Consumers will also have the right to individually request that a business disclose the categories and specific pieces of information that the business has collected about them and the purposes for collection, as well as any third parties to whom the business has sold or otherwise provided their information.

Right of Deletion

AB-375 also provides consumers with the right to be forgotten. Consumer will have the right "to request that a business delete any personal information about the consumer which the business has collected from the consumer." The expanded definition of "personal information" will extend this right to some profiling information related to consumers. However, a business may refrain from deleting a consumer's personal information if, among other reasons, the information is necessary to complete a transaction, comply with a legal obligation, or detect a security incident, among other exceptions.

Opt-In and Opt-Out Rights

The new law also provides consumers with greater control over their personal information. Importantly, the statute provides measures for consumers to restrict the sale of their personal information by: (i) restricting third parties that purchased a consumer's personal information from selling that information unless the consumer is provided explicit notice and is provided an opportunity to exercise the right to opt out; and (ii) restricting a business from selling a consumer's personal information unless the consumer has the right to opt out of the sale of his or her personal information. The new law precludes a business from discriminating against a consumer because the consumer exercised any of his or her rights.



The statute will impose significant changes on how businesses collect, store, sell, and otherwise process consumer personal information, significantly changing the data privacy legal landscape for large businesses in the United States.



The statute also restricts the sale of data collected from minors; data collected from children under 16

cannot be sold without opt-in consent from the consumer, if between 13 and 16 years old, or the parent or guardian, if under 13 years old.

Private Right of Action

A significant point of contention was the new mechanism for consumers whose data is included in a data breach to recover statutory damages, as it authorizes a private right of action for "[a]ny consumer ... whose nonencrypted or nonredacted personal information ... is subject to an unauthorized access and exfiltration, theft, or disclosure as a result of the business' violation of the duty to implement and maintain *reasonable security procedures and practices* appropriate to the nature of the information to protect the personal information...." (emphasis added). Consumers can recover damages of between \$100 and \$750 per incident, or actual damages, as well as seek injunctive or declaratory relief. This will require a business to evaluate the reasonableness of data security measures employed to protect personal information, or elect to deploy encryption more widely.

Enforcement

AB-375 directs the California Attorney General to solicit public participation for the purpose of adopting regulations, including expanding or refining the definition of "personal information" under the statute. Businesses are authorized to seek the advice of the attorney general on how to comply with the statute. The attorney general is authorized to enforce civil penalties of up to \$7,500 for each violation, with a portion of the penalty to go into the newly created "Consumer Privacy Fund."

The adoption of the new law indicates a new trend in the United States for stronger, comprehensive approaches to consumer data privacy, at least at the state level.

THREE KEY TAKEAWAYS

1. AB-375, California's new consumer privacy law, contains a broad definition of "personal information," even including "[i]nferences drawn from any of the [personal information] to create a profile about a consumer."
2. AB-375's "right to be forgotten" provision establishes that consumers will have the right "to request that a business delete any personal information about the consumer which the business has collected."
3. Enforcement provisions in AB-375 authorize California's state attorney general to enforce civil penalties of up to \$7,500 for each violation.



Daniel J. McLoon
Los Angeles



John A. Vogt
Irvine



Jeff Rabkin
San Francisco / Silicon Valley



Mauricio F. Paez
New York

[All Contacts >>>](#)

YOU MIGHT BE INTERESTED IN: [Go To All Recommendations >>](#)



[Jones Day Global Privacy & Data Security Update Vol. 18](#)



[DOJ's Business Email Compromise Takedown Illustrates Pervasiveness of Internet Fraud Schemes](#)



[U.S. Government Releases Report on IoT Botnets and Other Distributed Attacks](#)

SUBSCRIBE

SUBSCRIBE TO RSS



Jones Day is a global law firm with more than 2,500 lawyers on five continents. We are One Firm WorldwideSM.

Disclaimer: Jones Day's publications should not be construed as legal advice on any specific facts or circumstances. The contents are intended for general information purposes only and may not be quoted or referred to in any other publication or proceeding without the prior written consent of the Firm, to be given or withheld at our discretion. To request reprint permission for any of our publications, please use our "Contact Us" form, which can be found on our website at www.jonesday.com. The mailing of this publication is not intended to create, and receipt of it does not constitute, an attorney-client relationship. The views set forth herein are the personal views of the authors and do not necessarily reflect those of the Firm.