California Lawmakers Pass Sweeping New Data Privacy Law

LAST-MINUTE LEGISLATIVE COMPROMISE OPENS DOOR TO LIABILITY AND LITIGATION

Insights
6.29.18

Due to some last-minute bargaining between state lawmakers and proponents of a controversial data privacy initiative, California businesses will soon need to prepare to comply with a new state measure designed to protect private data of consumers. The new requirements take effect in 2020, but now is the time to begin the process of considering the applicability of these rules to your business and ensuring that your organization is in compliance.

So What Will The New Law Entail?
The new law—passed by the legislature and signed into effect by the governor late yesterday—will not go into effect until 2020, which means there could be follow-up measures that change or clarify certain provisions of the law before it goes into effect. As it stands now, however, the privacy provisions of AB 375 will apply to any business in the State of California that satisfies any of the following:

- Annual gross revenue over $25 million;
- Alone or in combination, annually buys, receives, sells or shares for commercial purposes the personal information of 50,000 or more consumers, households, or devices; or
- Derives 50 percent or more of its annual revenues from selling consumers' personal information.

Overall, AB 375 enacts fairly sweeping consumer privacy protections, including the following:

- **Disclosure** – Under the new law, consumers have the right to seek disclosure of any of their personal information a business has collected, up to twice a year. At or before the collection of the information, businesses have to inform consumers as to the categories of information collected and the purposes for which it will be used. The bill also provides consumers the right to request information about what types of information are being collected and any third parties the information is shared with.
- **Right to Delete Information** – The new law affords consumers the right to request deletion of any personal information a business collects. Businesses that collect personal information would need to disclose this right to delete to consumers. However, there are numerous exceptions to this requirement. For instance, businesses are not required to delete the information if it is necessary for the business or service provider to maintain the consumer's

personal information in order to "otherwise use the consumer's personal information, internally, in a lawful manner that is compatible with the context in which the consumer provided the information."

- **Right to "Opt Out" of the Sale of Personal Information** – Under the new law, consumers would have the right to opt out of the sale of their personal information. A business would have to abide by such a request and respect the request to opt out for 12 months before being permitted to request that consumer authorize the sale of personal information. The law defines "sale" to mean "selling, renting, releasing, disclosing, disseminating, making available, transferring, or otherwise communicating…a consumer's personal information by the business to another business or a third party for monetary or other valuable consideration."
- **Discrimination Provisions** – The law prohibits discrimination against a consumer based on the fact that the consumer exercised their rights under the new law. Such discrimination includes denying goods or services to the consumer, charging different prices or rates for goods or services, providing a different level or quality of goods or services to the consumer, and suggesting that the consumer will receive a different price or rate or a different level of quality of goods and services.
- **Policies and Procedures** – The law outlines requirements regarding how businesses should respond to requests and the timelines for doing so, and also provides guidance on how to comply with the various provisions, namely the process of identifying consumers and associating the information that is supplied by the consumer in the relevant request with information the business has collected that is actually connected to that person. The law also outlines specific pieces of information that would need to be included in the privacy policies of businesses that have such policies in place.
- **Enhanced Rights for Minors** – Businesses are prohibited from selling the information of minors without their consent. In other words, the new law provides an "opt-in" mechanism for minors, while other consumers have the ability to "opt out" of the sale of personal information.

California employers in particular will need to look at each of these requirements carefully and consult with legal counsel to evaluate their potential applicability to personal information regarding employees, in additional to such information they maintain regarding customers or other consumers.

Private Right Of Action For Data Breaches

One of the most troubling aspects of the new law creates a private right of action for any consumer for data breaches – apparently without any proof of injury.

The law provides that "any 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" may be subject to a civil lawsuit. A consumer would be

entitled to recover actual damages or statutory damages of between $100 and $750 per consumer per incident (whichever is greater), plus injunctive or declaratory or other relief.

This is similar to language contained in another legislative proposal that had been making its way through the legislative process, which we discussed here and here. That language was incorporated into the provisions of AB 375.

The private right of action provisions of AB 375 do make several accommodations to the business community, at least as compared to the language that was contained in the proposed ballot initiative.

First, a consumer would have to provide a business with written notice and a 30-day "right to cure" any alleged violation for statutory damages (but not actual damages): "In the event a cure is possible, if within the 30 days the business actually cures the noticed violation and provides the consumer an express written statement that the violations have been cured and that no further violations shall occur, no action for individual statutory damages or class-wide statutory damages may be initiated against the business."

Second, the consumer must notify the Attorney General within 30 days that an action has been filed. The Attorney General then has 30 days to either (1) notify the consumer that the Attorney General intends to prosecute an action in lieu of the consumer's private lawsuit, or (2) refrain from acting, allowing the consumer bringing the action to proceed. In addition, the law provides that the Attorney General can "notify the consumer bringing the action that the consumer shall not proceed with the action." This interesting language appears to give the Attorney General veto power over any pending civil action, regardless of whether they take over the case.

If all of this sounds too much like the Labor Code Private Attorneys General Act (PAGA) for comfort, you're on the right path—and it should raise alarm bells for California businesses. Despite some of the concessions described above, this language threatens to open the door to litigation against California businesses for data breaches under certain circumstances, where there may not have been a financial or other injury to the consumer.

Arbitration Provision Thrown In For Good Measure

AB 375 also contains language that states, "Any provision of a contract or agreement of any kind that purports to waive or limit in any way a consumer's rights under this title, including, but not limited to, ***any right to a remedy or means of enforcement***, shall be deemed contrary to public policy and shall be void and unenforceable."

This language clearly seems designed to prohibit arbitration clauses that would compel consumers to bring claims under the new law through arbitration as opposed to class action lawsuits.

What Comes Next?

The good news is that AB 375 does not go into effect until January 1, 2020. That means that you have time to analyze the requirements of the new law and plan ahead. In addition, because the bill was

put together in such a rushed fashion, legislative leaders hinted that there could be further legislative changes to some of these provisions. Moreover, the bill specifically charges the Attorney General with adopting regulations to implement the provisions of the law, which could provide more clarity for covered businesses.

But there are new complex requirements that may impact many facets of your operations, so you don't want to wait around until the last minute. You should begin the process of reviewing these new requirements and determining their potential applicability to your operations.

Most importantly, you should begin to get a handle on the types and scope of data you currently collect (and have collected already and stored) that may be covered by the law. You should start assessing your current policies and procedures now so you are not caught short when the law goes into effect.

If you have any questions, contact your Fisher Phillips attorney, an attorney in any of Fisher Phillips' five California offices, or any member of the firm's Privacy and Cyber Practice Group.

This Legal Alert provides an overview of a specific state law change. It is not intended to be, and should not be construed as, legal advice for any particular fact situation.

Related People

Risa B. Boerner, CIPP/US, CIPM
Partner
610.230.2132
Email

Benjamin M. Ebbink
Partner
916.210.0400
Email

Service Focus

Privacy and Cyber