BCLP. Client Intelligent

RetailLawBCLP

CALIFORNIA ENACTS SWEEPING PRIVACY LEGISLATION CONCERNING CONSUMERS' PERSONAL INFORMATION

Jun 29, 2018

California enacted privacy legislation yesterday that is the first of its kind in the United States and moves California law closer to the protections afforded in the European Union by the General Data Protection Regulation (GDPR). The law also creates a private right of action to pursue a lawsuit against a company arising out of a breach of personal information, which will likely give rise to a substantial increase in data breach lawsuits in California. There is a lot to unpack in this new piece of legislation, which spans 28 pages and will engender various regulations before its January 2020 effective date. The new law forestalls possibly more onerous requirements from a citizen ballot initiative.

Following is a breakdown of the new California Consumer Privacy Act of 2018.

How is this like the GDPR?

Like the GDPR, the California law defines "personal information" far more broadly than seen before in the U.S., bringing it in line with the GDPR definition. It 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. There are many examples identified, including internet search history, employment-related information, and information associated with protected classes under California law (*e.g.*, race, gender). This definition is very similar to the GDPR's view of personal information – *i.e.*, can we link the data element to an actual person? If so, it's personal information.

Here is a summary of a few key requirements:

- **Right to access information:** Up to twice a year, a consumer can request that a business provide it with the *specific pieces of information* the business has collected about them, including the categories of information sold for each third party to whom it is sold, the sources of collection, and the business purpose for collection.
- **Right to deletion:** A consumer can request that a business delete the personal information collected from the consumer about them, although this is subject to numerous exceptions,

including business necessity.

- **Right to opt out of sale of personal information:** Individuals over the age of 16 will have a right to opt out of the sale of their personal information via a clear and conspicuous link on businesses' internet home page titled "Do Not Sell My Personal Information"
- **Affirmative opt in for sale of minors' information:** Businesses will have to obtain affirmative consent prior to sale of minors' personal information.
- **Prohibition against different rates or levels of services:** Businesses will be prohibited from discriminating against a consumer for opting out of the sale of their personal information by charging different rates or prices or providing a different level of quality of goods or services, while still permitting the business to offer incentives for collection of personal information
- **Online disclosure:** The rights must be disclosed in the business's online privacy policy (note that CalOPPA, the existing California law requiring certain privacy policy disclosures, already contains several requirements).

What's in the GDPR that is Missing from the CA law?

Unlike the GDPR, which applies to companies of all shapes and sizes established in the EU or offering goods and services to persons in the EU, the California law only applies to business with gross revenues in excess of $25 million, personal information data brokers, and companies deriving 50 percent or more of their annual revenue from selling consumers' personal information. In other words, bigger companies and tech companies that offer free goods or services in exchange for collection of your personal information and the right to sell it will be the ones most likely to be impacted. It also doesn't apply to data regulated by HIPAA or the GLBA.

Unlike the GDPR, the California law **does not** require: (a) the creation of a data protection officer position, (b) more onerous breach reporting requirements, like the 72 hour supervisory authority notification requirement in the EU, or (c) specific contractual provisions to be in place between businesses and their service providers.

How much time do I have to comply with requests for information?

Businesses will have 45 days to comply with requests for information, although a business may unilaterally extend the response period another 45 days with notice to the consumer.

If I violate the law, what are the consequences?

Enforcement of violations relating to the above requirements is left solely to the California Attorney General. A business is in violation of the law if it fails to cure any alleged noncompliance within 30

days of notification, and can be subject to up to $7500 in civil penalties for each violation.

What is the change concerning data breaches?

Perhaps the most dramatic departure from existing law can be found in section 1798.150, which provides consumers with a private right of action when their personal information has been breached. This provision was passed to address what has previously been an often insurmountable hurdle to data breach lawsuits – establishing standing or showing harm when there has been no identity theft resulting (yet) from the data loss. The new law provides that an individual can recover the greater of actual damages or between $100-750 in statutory damages, to be determined by the court based on a number of factors, including misconduct by the business and willfulness of behavior, along with the business's assets and net worth.

Fortunately, the statute adopts the more narrow definition of personal information found in the existing data breach notification law, which covers: name in combination with social security number, driver's license or California ID number, financial account information with an access code, medical information, health insurance information, or username and email in combination with a passcode or security question answer for an online account.

Before suing, the consumer would have to give the business notice and an opportunity to cure, but in a breach where data has been lost, it's hard to envision how a cure would be possible. If a business provides free credit monitoring, is that considered a "cure?" This provision likely will give rise to many more questions.

Within 30 days of bringing an action, the consumer has to notify the California Attorney General's office of the suit, who may either: (1) notify the consumer of their intent to bring suit within 6 months; (2) refrain from acting thereby permitting the consumer to continue the suit; or (3) notify the consumer that they can't continue the suit. This provision mirrors that of Prop 65, the California law that requires warning consumers about exposures to certain chemicals. Effectively, the Attorney General only intervenes in such actions if there's a public policy issue involved, so businesses should not expect much relief from this provision.

What do I do now?

Since the law will not be effective until January 2020, and regulations implementing it are expected to be issued, companies who will be impacted would be wise to begin examining where they maintain personal information about California residents and their ability to provide timely responses to requests for information about that data. Companies will need to build out compliance processes for handling requests in a timely manner. In addition, companies would be well served to ensure they are prepared in the event of a data breach, including creating an incident response plan and rehearsing mock breaches with the incident response team. In light of the statutory damages, it will be important to show that the business took data security seriously and responded quickly and appropriately in the event of a breach.

For more information, contact the author, or any member of our Retail or Data Privacy teams.

RELATED PRACTICE AREAS

- Retail & Consumer Products

MEET THE TEAM

Merrit M. Jones

San Francisco

merrit.jones@bclplaw.com
+1 415 675 3435
