Updates
June 29, 2018
California Consumer Privacy Act of 2018 Brings Some GDPR Aspects Stateside

On June 28, 2018, California adopted the strictest general privacy and data security law in the country, called the "California Consumer Privacy Act" (codified in Assembly Bill 375), which will come into effect on January 1, 2020. This is the first installment of two updates covering the act. We focus here on the main aspects of the law, and a more in-depth analysis is forthcoming in the second part of this series.

As an overview, this law, as written, will transform how companies that handle consumer data do business in California.

The act will require businesses to notify consumers about the type of data they collect, both in privacy policies and in response to specific requests, and provide consumers the option to opt out of the data being utilized for certain purposes. The act will also provide a limited private right of action for violations and statutory damages, including for data breaches resulting from lack of reasonable security.

California, already a popular venue for plaintiffs to file consumer privacy class action litigation, may likely see an increase when the act becomes effective. And even if litigation is not filed, compliance costs are likely to be significant. As one example, the act significantly expands the definition of personal information, like the new EU privacy law called the General Data Protection Regulation (GDPR) does, to include unique identifiers, and also to include broad biometric information, inferences drawn from other information, and other categories. In so doing, the act will impose more stringent privacy standards on digital advertising and analytics, which are commonly associated with new technologies.

The legislation is the result of a last-ditch effort to have a stricter ballot measure withdrawn, and it passed on the last day for the withdrawal of that initiative. Unlike a ballot measure, the new privacy rules in the form of legislation can more easily be changed by lawmakers. The act also has a later effective date than the ballot measure. Accordingly, with some time remaining before the new law goes into effect, we may see changes to the final version prior to actual implementation. There could also be federal efforts to pass a broader bill, similar to the passage of the CAN-SPAM Act years ago in response to California's junk email statute.

The New California Consumer Privacy Act of 2018

The California Consumer Privacy Act of 2018 is the most comprehensive general data privacy bill of its kind to pass in the United States. The main focus **is on greater regulation of personal information collected and sold by companies, and on breaches of such information where reasonable security measures have not been taken**. The preamble of the law highlights the increasing amount and use of data in our highly digitized economy, though the act is not limited to digital data. The act will apply to for-profit companies doing business in California that collect consumers' personal information and exceed $25 million in gross revenue; handle the personal information of 50,000 or more consumers, devices or households; or derive more than 50% of their annual revenue from selling consumers personal information.

The act states, among other things, that California law has not kept pace with developments in tracking or otherwise collecting information. The act contains several relevant provisions in this regard, some of which resemble the GDPR.

First, the act provides consumers a right to know the categories and specific pieces of personal information that a business has within the past year collected, sold to a third party, or disclosed to another person for a business process. Personal information is very broadly defined, including, among other things, unique personal identifiers,

IP addresses and "inferences drawn from" personal information. This expansion would shift current thinking and may likely require reassessment of ways personal information is handled by companies using such information. Businesses would need to provide California consumers with a means to make such requests and honor verifiable requests within 45 days.

While this proposal also bears some resemblance to California's Shine the Light law, the requirements are more detailed and more inclusive. For example, California's Shine the Light law does not include unique identifiers in the definition of personal information while the California Consumer Privacy Act does. Thus, businesses may be required to have more detailed records than they currently do about when/how personal data is collected, shared and sold, and may also need to implement processes for sharing information about the categories and the actual data collected. While the act does not explicitly call for recordkeeping (like the GDPR does), companies may feel that they need to create such a data inventory in order to respond to requests and meet the deadlines imposed by the 45-day response requirement.

Second, under the act, consumers can also request that a business not sell their personal information, and companies would be limited in how they could treat consumers differently for opting out of selling their information. This bears some resemblance to the GDPR, which prohibits companies from making consent to process data a condition of using their service. Notably, conditional consent is one of the issues that has spawned consumer advocate claims in the first wave of GDPR collective actions. The act also prohibits businesses from selling the personal information of individuals under 16 years old unless they affirmatively authorize such sharing, referred to as the "right to opt in."

Third, the act requires businesses to make various disclosures in their privacy policies, including:

1. A description of a consumer's rights pursuant to the act;

2. One or more methods through which consumers may submit requests to the business;

3. A list of the categories of personal information collected in the preceding 12 months;

4. Lists of the categories personal information sold or disclosed to third parties in the preceding 12 months, or a statement that such information has not been sold; and

5. A link titled "Do Not Sell My Personal Information" that allows consumers to opt out of the sale of their personal information without having to create an account.

Fourth, the act provides a limited private right of action for plaintiffs to institute a civil action seeking damages or relief for the failure to maintain reasonable security measures in the event of unauthorized access and exfiltration, theft or disclosure of nonencrypted or nonredacted personal information. The right of action requires the consumer to first give the business 30 days' written notice to cure their violation, and give notice to the California attorney general who decides whether to prosecute or allow the consumer to proceed. Once both conditions have been met, a consumer may then seek to recover damages in a minimum of $100 and maximum of $750 per incident (or actual damages, whichever is greater).

The act also provides that violations are actionable by the California attorney general under the state's Unfair Competition Law after a 30-day period in which the business has the opportunity to cure the violation. In addition, the act authorizes a civil penalty of up to $7,500.

Fifth, the law allows consumers the right to request deletion of their personal information that a business holds, and the business is required to honor the consumers verified request absent an exception.

The California law will impose substantial new compliance requirements on businesses when it becomes effective in 2020.

What Should Your Business Do Now?

The act is not in effect yet. However, there are several things companies should consider now, as best practices that will be helpful to prepare for the new law:

1. Consider working with legislators and the attorney general to address issues in interpretation well in advance of the effective date.
2. Consider conducting a privacy assessment to understand how personal data, as newly defined, is collected, used, disclosed and/or sold, and better position your company for compliance.
3. Understand that the act applies to all companies doing business in California that meet the above thresholds and collect personal information from consumers, and if you are engaged in digital advertising or use analytics to monitor adoption or use of your website, mobile app or IoT device, the act will apply to this ad tech activity, just as the GDPR does. Accordingly, a conversation with your digital marketing teams regarding their data collection, sharing and storage practices would be good to include as part of your overall data inventory practices.
4. Consider technological changes that will need to be made in order to comply with the law and lead times required to implement such changes.
5. Consider the feasibility of creating a process to accommodate California access requests, including creating an online portal.
6. Consider if and how third-party agreements will need to be restructured to address the act.
7. Consider internal training well in advance of the effective date to prepare for compliance.

Please look for the second update in this series in which we take a deeper analytical dive into the new California law.

Authors

Explore more in

Privacy & Security | Litigation | Advertising, Marketing & Promotions | Retail & Consumer Products

Related insights

Update

California Court of Appeal Casts Doubt on Legality of Municipality's Voter ID Law

Update

February Tip of the Month: Federal Court Issues Nationwide Injunction Against Executive Orders on DEI Initiatives