At Rocket Speed – The California Consumer Privacy Act of 2018 Signed into Law Yesterday

June 29, 2018

While U.S. companies focused on the imposition of burdensome data protection laws being implemented overseas, California was hard at work on revamping its own laws. As of June 25, 2018, the home of big technology, Silicon Valley, Facebook, and Google, was prepared to consider the California Consumer Personal Information Disclosure and Sale Initiative ("Initiative") on the November 2018 ballot. The Initiative sought to enact a version of the California Consumer Privacy Act of 2018, requiring businesses to disclose, on a consumer's demand, the personal information a business collects, the purpose for which it is used, and to whom it is sold or shared with. The Act also allows individuals to restrict the sharing of their information. Finally, the Act provides a simple path to recovery for violations. Although companies like Facebook and Google dropped their opposition to the Initiative, concerns remained among the business community, so California lawmakers stepped in.

On June 21, 2018, in anticipation of the Initiative qualifying for the November 2018 ballot, lawmakers revived stalled bill AB 375, a version of the California Consumer Privacy Act of 2018 that had been pending since February 9, 2017. On June 25, 2018, the California Senate offered an Amended AB 375 seeking to strike a compromise between the Initiative and concerns of the business community. Lawmakers had just three days to consider, pass, and get AB 375 to the Governor's desk.

Sweepingly, the California Consumer Privacy Act of 2018 was signed into law yesterday afternoon, effective January 1, 2020. This Act changes the landscape and sets a new tone for data protection in the United States. Notably, companies are cautioned not to be misled by the word "Consumer" in the title of the Act, as the term is broadly defined as "a natural person who is a California resident…." The Act also outlines five privacy rights of Californians to: (1) know what personal information is being collected; (2) know whether their information is being disclosed and to whom; (3) opt-out of having their information shared; (4) access their personal information; and (5) receive equal service on exercise of their privacy rights. These rights are extensive and are certain to impact even businesses whose primary focus is not data collection:

1. **The Right to be Forgotten.** One of the more salient points of the Act is its expansion of the right to be forgotten beyond personal information of minors. The Act requires compliance not only from the business with which the consumer has the relationship to process the deletion request but also from any third-parties with whom the consumer's information was shared. In addition, the Act has a data portability requirement obligating businesses to provide consumers with their personal information in a format that will allow them to transmit it to another entity without hindrance.
2. **Verifiable Consumer Requests.** The Act allows consumers to submit up to two verifiable consumer requests a year, free of charge, which may request access: to their personal information held by the business, to have their information provided to them in a portable format, and to have their information deleted. Businesses will have 45 days to respond to the request and must provide at a minimum a toll free number and website address through which consumers can submit their request.
3. **Disclosures, but not Affirmative Consent.** The Act requires less specific disclosures than the Initiative would have—and requires business to disclose, at the time of collection, the categories of personal information collected, and the purposes for which information is being collected. However, upon the consumer's request, businesses are required to disclose the categories and specific pieces of personal information collected, the sources from which personal information was collected, the purposes for collecting or selling personal information, and the categories of third-parties with whom personal information is shared.
4. **Applies to California Residents and Only Certain Businesses.** The obligations and rights under the Act only apply with respect to California residents and only applies to businesses that "do business in the State of California" and need meet only one of three criteria: (1) derives 50% or more of its annual revenue from selling personal information; (2) has annual gross revenue in excess of $25,000,000; and (3) buys, receives, sells, or shares the personal information of more 50,000 or more consumers, households or devices on an annual basis.

5. **Expands the Definition of Personal Information.** It expands the definition of personal information under California law from certain categories of information to "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."
6. **Restrictions on Minor's Personal Information.** The Act only requires affirmative consent with respect to the sale of personal information of minors. Consent from a minor's parent is required for those under the age of 13. Affirmative consent must be received from the minor if between the ages of 13 and 16.
7. **Right to Opt-out.** Consumers must be given the opportunity to opt-out from their personal information being sold or shared with third-parties and may not be discriminated against through a change in the quality or pricing of services unless the difference is reasonably related to the value provided by the sharing of the consumer's data.
8. **Restrictions on Third-Parties.** Third-parties who receive or buy personal information must provide consumers the same opportunity to opt-out of the further selling or sharing to further parties.
9. **Duty to Implement Reasonable Security Measures.** The Act adopts the "privacy by design" position taken by recent data protection laws around the world and requires businesses to "implement and maintain reasonable security procedures and practices appropriate to the nature of the information…."
10. **Enforcement and Lawsuits.** The Act allows enforcement of violations through private right of actions or actions brought by the Attorney General. The Initiative sought to have the private right of action apply to any violation under the Act, but the Legislature compromised and limited actions to incidents involving a breach of information. The Act also lowers the statutory damages from the $1,000 to $3,000 proposed in the Initiative to $100 to $750.

The new obligations under the Act highlight the need for companies to take a holistic approach to data protection, such that it is able to harmonize the various data protection schemes developing across the nation and around the world that may be applicable to its operations. Although the Act may seem to be of limited application, businesses may have a hard time avoiding its application in sectors where they cannot choose their own customers (or website visitors). Further, although the statutory damages may seem small compared to other regulatory fines, a typical violation may impact hundreds or thousands of customers which can drive large exposures. Businesses should also bear in mind that California is a state that allows private attorney general actions brought by individuals in the name of the state. This vastly increases the chances of litigation. Finally, even though January 1, 2020, may seem distance in the future, companies are cautioned that compliance with this Act will require time consuming operational changes. Therefore, companies should consider taking steps to implement these changes now.

Dykema's Privacy and Data Security group routinely helps both domestic and international clients not only address the pressing issues of today, but also anticipate and plan for swift regulatory changes. If you have questions on how California's Consumer Privacy Act of 2018 may impact your organization, please contact Cinthia G. Motley (cmotley@dykema.com), Ashley S.A. Jackson (ajackson@dykema.com), or your Dykema relationship attorney.

Attorneys

Cinthia Granados Motley

Dante A. Stella

Practice Areas

Privacy and Data Security