Proskauer

The California Consumer Privacy Act of 2018

Privacy Law Blog on **July 13, 2018**

This has been a big year in the data protection world, with the headline-grabbing General Data Protection Regulation (GDPR) occupying most of the spotlight with its plethora of privacy-related requirements and potential for high fines for violators. While companies (justifiably) may be focused on the GDPR at the moment, it's also important to keep an eye on new privacy laws on the horizon in order to avoid last-minute scrambles for compliance as effective dates near. Foremost among these new laws is the California Consumer Privacy Act of 2018. The Act was introduced and signed quickly in order to prevent voters from facing a similar ballot initiative in the November election. This post provides an overview of the new law, which will go into effect beginning January 1, 2020.

What is the California Consumer Privacy Act of 2018?

The California Consumer Privacy Act of 2018 (the "Act") was signed into law by California Governor Jerry Brown on June 28, 2018, after being hastily introduced in the California Legislature just a few days prior. Why all the rush? It all stems from California's rather unique ballot initiative process, which is worth explaining in more detail.

In California, the power to introduce legislation is not just limited to politicians. Under California law, citizens can propose new laws and constitutional amendments, and may secure a statewide vote on their initiatives if they get enough signatures on a petition advocating that the proposed law appear on a future ballot. The proponents of an initiative begin by circulating a petition, and once the requisite number of signatures are qualified by the Secretary of State, the initiative is approved to appear on the upcoming ballot. If approved by California voters, the initiative becomes state law – but once enacted, it cannot be amended by the state legislature. Instead, any amendments generally must be made through other initiatives. Practically speaking, that means it can be very difficult to amend ballot initiatives once they are voted into law.

Here, the California Legislature was eager to pass the Act because doing so would prevent Californians from voting on a similar initiative that was slated to appear on the ballot in the November 2018 general election. The initiative to implement the ballot measure collected some 629,000 verified signatures and was slated to appear on the ballot in November alongside other initiatives (including one proposing the division of California into three states, as well as measures pertaining to the regulation of kidney dialysis clinics and farm animal confinement, among others). However, the sponsors of the ballot initiative stated that they would withdraw the proposed measure from the ballot if the California Consumer Privacy Act was passed and signed by the Governor by June 29. Legislators took advantage of that option and hastily drafted and passed the Act just in time to meet the deadline.

The Act is seen by some as preferable to the ballot initiative because it provides mechanisms to refine its privacy-related requirements in the future, which makes it easier to amend the Act as opposed to a ballot measure voted into law via the initiative process. However, as described below, that does not mean that compliance with the Act will be a quick and painless process; instead, it's likely that many companies will find the compliance process as much of a struggle as their GDPR compliance efforts.

What are the Act's major provisions?

The Act (the full text of which is available here) gives "consumers" (defined as natural persons who are California residents) four basic rights in relation to their personal information:

1. the right to know, through a general privacy policy and with more specifics available upon request, what personal information a business has collected about them, where it was sourced from, what it is being used for, whether it is being disclosed or sold, and to whom it is being disclosed or sold;
2. the right to "opt out" of allowing a business to sell their personal information to third parties (or, for consumers who are under 16 years old, the right not to have their personal information sold absent their, or their parent's, opt-in);
3. the right to have a business delete their personal information, with some exceptions; and
4. the right to receive equal service and pricing from a business, even if they exercise their privacy rights under the Act.

The Act’s provisions are designed to put these rights into practice. The Act requires that companies make certain disclosures to consumers via their privacy policies, or otherwise at the time the personal data is collected. For example, businesses need to disclose proactively the existence and nature of consumers’ rights under the Act, the categories of personal information they collect, the purposes for which that personal information is collected, and the categories of personal information that it sold or disclosed in the preceding 12 months. In terms of compliance, these provisions will require companies to determine what personal data they are collecting from individuals and for what purposes, and to update their privacy policies every 12 months to make the disclosures the Act requires.

Companies that sell consumer data to third parties will need to disclose that practice and give consumers the ability to opt out of the sale by supplying a link titled “Do Not Sell My Personal Information” on the business’s home page. This is known as the right to “opt out.” The Act further provides that a business must not sell the personal information of consumers younger than 16 years of age without that consumer’s affirmative consent (or, for consumers younger than 13 years of age, without the affirmative consent of the consumer’s parent or guardian). This is known as the right to “opt in.”

Consumers also have the right to request certain information from businesses, including, for example, the sources from which a business collected the consumer’s personal information, the specific pieces of personal information it collected about the consumer, and the third parties with which it shared that information. The Act requires businesses to provide at least two means for consumers to submit requests for disclosure including, at minimum, a toll-free telephone number and Web site. Additionally, businesses will have to disclose the requested information free of charge within 45 days of the receipt of a consumer’s request, subject to possible extensions of this time frame. Companies therefore will need to determine how they can monitor their data sharing practices and marshal the requested information within a short period of time pursuant to a data subject’s request.

The Act also forbids businesses from “discriminating” against consumers for exercising their privacy rights under the Act. More specifically, that means businesses cannot deny goods or services, charge different prices for goods or services, or provide a different quality of goods or services to those consumers who exercise their privacy rights. However, the Act does permit businesses to charge a different price, or provide a different level of service, to a customer “if that difference is reasonably related to the value provided to the consumer by the consumer’s data.” How this confusingly-worded loophole will be interpreted remains to be seen.

It also is worth noting that businesses are permitted to offer financial incentives to consumers for the collection, sale, or deletion of personal information, subject to specific conditions and notice requirements.

What qualifies as “personal information” under the Act?

For purposes of the Act, “personal information” is defined as “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.” The Act provides a non-exhaustive list of examples that includes some expansive examples. For example, personal information includes “commercial information” (including “records of personal property, products or services purchased, obtained or considered, or other purchasing or consuming histories or tendencies”), “Internet or other electronic network activity information” (such as browsing and search histories), “education information” and “[a]udio, electronic, visual, thermal, olfactory, or similar information.” Personal information does not include information that lawfully is made available from federal, state or local government records that is used for a purpose that is compatible with the purpose for which such data is so maintained.

While various California laws define “personal information” in different ways, they generally recognize that “personal information” is information that can be used to identify a particular individual. The Act’s definition is worded more broadly, and includes information that is identifiable to a household, not necessarily a consumer. Also, the Act’s many examples of personal information serve to illustrate how wide-ranging the definition can be. For example, the definition of personal information includes unique personal identifiers, which is defined broadly to include device identifiers, other online tracking technologies and “probabilistic identifiers” (identifiers based on personal information that “more probable than not” identify a consumer or device). On the other hand, the Act does not apply to de-identified personal data, as long at the de-identification measures meet the Act’s very strict standards, or to aggregate consumer information, which also is defined strictly by the Act. Companies developing their compliance strategy should give careful consideration to the types of personal information they collect, and cast a wide net in terms of thinking about data that may fall within the Act’s definition.

Who has to comply with the Act?

The Act will apply to for-profit businesses that collect and control California residents’ personal information, do business in the State of California, and: (a) have annual gross revenues in excess of $25 million; *or* (b) receive or disclose the personal information of 50,000 or more California residents, households or devices on an annual basis; *or* (c) derive 50 percent or more of their annual revenues from selling California residents’ personal information. The Act also draws in corporate affiliates of such businesses that share their branding. That means that not-for-profits, small companies, and/or those that do not traffic in large amounts of personal information, and do not share a brand with an affiliate who is covered by the Act, will not have to comply with the Act.

A company also is exempted from its compliance obligations under the Act "if every aspect of … commercial conduct takes place wholly outside of California," meaning that: (1) the business collected the information from the consumer in question while he or she was outside California, (2) no part of any sale of his or her personal information occurred in California, and (3) no personal information collected while the consumer was in California is sold. Realistically, though, many companies will remain subject to the Act by virtue of having "consumers" (California residents) among their customers, as described in further detail immediately below.

Who is protected by the Act?

The Act requires that the protections listed above be made available to "consumers," who are defined as California residents for tax purposes. However, California's large population and economic presence means that many (if not most) companies serve California consumers – even if those companies have no physical presence in the State. Additionally, few companies are likely to cabin all of the Act's requirements to California residents, as it is difficult to offer a different Web site experience to residents of a specific state. For example, few companies are likely to devote the resources necessary to provide the Act's opt-out options to a user visiting a Web site from an IP address in California, while providing a Web site without those features to residents of the other 49 states. Realistically, this makes it likely that companies with California-based customers – which is most U.S. companies that have an online presence – will need to comply with the Act, and will need to update their privacy policies and Web sites in order to do so. They also will need to implement a means of expeditiously providing the disclosures required by the law.

How will the Act be enforced?

The Act can be enforced by the California Attorney General, subject to a thirty-day cure period. The civil penalty for intentional violations of the Act is up to $7,500 per violation.

The Act also provides a private right of action that allows consumers to seek, either individually or as a class, statutory or actual damages and injunctive and other relief, if their sensitive personal information (more narrowly defined than under the rest of the Act) is subject to unauthorized access and exfiltration, theft or disclosure as a result of a business's failure to implement and maintain required reasonable security procedures. Statutory damages can be between $100 and $750 per California resident per incident, or actual damages, whichever is greater. However, it is not obvious what "per incident" means in this context, so the ceiling for statutory damages currently is unclear.

A consumer who wishes to bring an action under the Act will need to jump through a few hoops before he or she can proceed with a claim. A consumer seeking statutory damages must provide the defendant business with thirty days' notice of his or her intent to sue before filing an action. (Consumers seeking actual damages do not need to supply such notice.) If the business provides the consumer with an "express written statement" demonstrating that the violation has been cured, and that no further violation will occur, within thirty (30) days of receiving the consumer's notice, then the consumer cannot proceed with his or her action for statutory damages. A consumer who files an action must provide notice to the Attorney General within 30 days after filing. The Attorney General may (1) respond by notifying the consumer that the Attorney General will prosecute the action instead, (2) respond by notifying the consumer that he or she must not proceed with the action, or (3) not respond at all within 30 days, thereby allowing the consumer to proceed with the action.

When will the Act become effective?

The Act will take effect on January 1, 2020.

How similar is the Act to the EU's GDPR?

Put simply: not that similar, although they do share some general features. Both the Act and the GDPR apply to companies located outside their borders, emphasize some of the same broad themes (such as the importance of access and transparency), and – perhaps most importantly – will require companies to expend a great deal of effort and resources to achieve compliance. However, that's really where the similarities end, as the laws' actual provisions overlap but are also quite different.

Perhaps the most basic difference is the fact that the GDPR is an omnibus law, while the Act is not. Not only does the GDPR regulate what disclosures companies must make to data subjects, it also covers procedures for data breach notification to individuals and regulators, data security implementation, cross-border data transfers and more. The Act is more limited, as it primarily is concerned with consumer privacy rights and disclosures made to consumers.

Both the GDPR and the Act give consumers certain rights as to their personal data, but those rights differ somewhat. While both the GDPR and the Act grant users the right to know what personal information a company has about them, Articles 15 and 20 of the GDPR impose additional requirements as to which data must be shared with the user, and the manner in which the disclosure must be made. Further, the GDPR offers a variety of additional rights to data subjects, including the right to be forgotten, the right to rectification, and the right to not be subject to a decision based solely on automated processing – none of which appear in the Act.

All that being said, the fact that the Act is less comprehensive than the GDPR does not mean the Act itself has a narrow scope, or that it can be overlooked. Make no mistake – the Act's sweeping nature should not be underestimated, and will require companies to expend a great deal of effort to achieve compliance.

It also is important to note that the GDPR does not subsume the Act, and that compliance with the GDPR does not ensure compliance with the Act. Most significantly, the two laws offer different – and potentially conflicting – approaches to consumer consent. The GDPR forbids companies from collecting, processing, or transferring personal information without a legal basis, and recognizes that user's informed and unambiguous consent may provide that legal basis. However, "opt out" mechanisms, such as pre-ticked check boxes, are not viewed as a means of obtaining valid consent under the GDPR. Instead, users must "opt in" to give their consent, such as by clicking on an unchecked box marked "I Agree" to indicate that they assent to the collection and use of their personal data. Unlike the GDPR, the Act does not require companies to obtain user consent to their processing of consumers' personal information. Instead, it requires business to offer consumers the opportunity to "opt out" of one specific use of their data: the *sale* of their personal information (except for minors under the age of 16, for whom consent must be given affirmatively). In short, the GDPR precludes the use of an "opt out" as a means of determining what may be done with users' personal information, while the Act requires the use of an "opt out" to prevent the sale of user data.

This marked difference between the GDPR and the Act presents a potential quandary for companies subject to both laws. Specifically, a company that sells its customers' personal data to third parties potentially may have to implement both opt-in and opt-out mechanisms in order to legally sell that data. If the company relies on user consent in order to sell or otherwise transfer the personal information of their EU customers to third parties, the company will have to implement the appropriate opt-in mechanisms for its customers in the EU. However, that same company will have to implement an opt-out mechanism to allow their California customers to prevent the sale of their personal information. Navigating compliance is likely to prove tricky for companies in this position. They may choose to find a legal basis other than consent in order to process EU user data, they may direct EU users to a Web site with an opt-in option and California (or more likely U.S.) users to a site with an opt-out function, or they may find another solution. Regardless, companies in this position will need to give some thought to their compliance strategies.

What is the potential impact of the Act?

As a practical matter, this law has the potential to change the privacy law landscape in the U.S. – not just California. As described above, the law's protection of California-based "consumers" means that many companies, even those based outside California and even outside the U.S., will be subject to its requirements. Businesses will incur significant compliance costs in order to update procedures, policies and Web sites in accordance with the new law. Additionally, the Act's grant of a private right of action means that companies will have to anticipate a possible flood of consumer-driven litigation.

We expect that the state legislature will continue to refine and amend the Act's privacy-related requirements before the final version of the law goes into effect on January 1, 2020.

Companies should start formulating compliance strategies well before the law goes into effect January 1, 2020. In the meantime, check back here for additional updates and guidance related to the Act.

Special thanks to summer associate Casey Harless for her contributions to the blog.

View Original