August 22, 2018 | Insights, Litigation & Dispute Resolution

# California Enacts Innovative Consumer Privacy Law

By: Rich May, Arvid von Taube

On June 28, 2018, just days after being introduced into the California Legislature, Governor Jerry Brown signed into law the California Consumer Privacy Act of 2018 (the "Act"). The Act goes into effect on January 1, 2020, although amendments are possible before then.

The Act gives fundamental privacy rights to California residents with respect to how certain companies doing business in California handle personal information.

## WHO DOES THE ACT REGULATE?

The Act applies to all for-profit companies that (1) do business in the State of California, (2) collect personal information of California residents and (3) meet one of the following criteria: (a) have annual gross revenues in excess of $25 million, (b) annually buy, receive for commercial purposes, sell or share for commercial purposes, the personal information of 50,000 or more California residents, households or devices or (c) derive 50% or more of their annual revenues from selling California residents' personal information.

The Act specifically excludes those companies whose commercial conduct takes place entirely outside the State of California and those companies that operate on a not-for-profit basis. The Act assumes that all commercial conduct occurs outside the state if (1) the business collected the personal information from the California resident 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.

## WHO DOES THE ACT PROTECT AND WHAT ARE THEIR RIGHTS?

The Act protects any natural persons who are California residents for tax purposes. The Act gives those persons the following basic rights with respect to personal information:

### Related Services

Litigation & Dispute Resolution

### Related Attorneys

Arvid von Taube

 

- **The right to know what personal information is being collected about them.** The regulated company must disclose to the resident the categories of personal information that are collected and the purpose for which such personal information is used. Such company cannot collect information outside of those categories disclosed to the resident.
- **The right to know whether their personal information is sold or disclosed and to whom, and the right to opt out of such sales or disclosures.** This information must be provided to the resident free of charge and may be delivered by mail or electronically.
- **The right to request that the company delete any personal information about the resident that the company has collected from the resident.** The Act provides for certain exceptions to this requirement, such as allowing the company to retain the information to complete the transaction or perform a contract for which the information was collected, to comply with other applicable laws, or internal use in a lawful manner that is compatible with the context in which the resident provided the information.
- **The right to receive equal service and price, even if the resident exercises his or her privacy rights under the Act.** However, this does not prohibit a company from charging a resident a different price or rate, or from providing a different level or quality of goods or services to the resident, if that difference is reasonably related to the value provided to the resident by the resident's data.

## WHAT IS PERSONAL INFORMATION?

The Act defines personal information as any 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" and includes a non-exhaustive list of examples such as name; alias; postal address; unique personal identifier; Internet Protocol address; email address; account name; social security number; driver's license number; passport number; commercial information, including records of personal property; products or services purchased obtained, or considered, or other purchasing or consuming histories or tendencies; biometric information; internet or other electronic network activity information, including, but not limited to, browsing history, search history, and information regarding a consumer's interaction with a website, application, or advertisement; geolocation data; audio, electronic, visual, thermal, olfactory, or similar information; and professional or employment-related information.

However, California residents should be aware that personal information does not include any information that is lawfully made available from federal, state or local government records. For example, if a resident includes his email address on a filing made with a

 

governmental entity and that filing shows up on a docket that is available for searching by the public on the web, the email address would presumably no longer be protected by the Act. As of the publication of this blog post, the State of California has not adopted any regulations to help interpret the Act, but those will be forthcoming and may address how personal information can lose, and correspondingly regain, its protected status.

## WHAT ARE THE PRACTICAL IMPLICATIONS FOR A COMPANY LOCATED OUTSIDE OF CALIFORNIA?

Unless a business outside of the State of California does not meet the applicability thresholds or is certain that it has no contact with California residents, it should seek to comply with the Act. The good news is that if such business has already undertaken to comply with the European Union's new General Data Protection Regulation (the "GDPR"), a lot of the required changes may already be in place. Please review our recent blog post on the GDPR for those recommendations, which include creating or updating privacy policies to clearly state what information is collected from users and for what purpose, creating an opt-in system for collection of data, and tracking such data by user for opt-out and deletion requests.

There are two ways that a company can be punished for failure to comply with the Act. The first is by the California Attorney General, who can enforce violations, subject to a thirty day cure period, with a penalty of up to $7,500 per violation. The second is by a resident who can bring a private right of action under the Act seeking statutory damages ranging from $100 to $750 per incident, or actual damages suffered. An "incident" isn't defined under the Act so it is unclear what the actual monetary ceiling might be. However, before a resident may file a private lawsuit under the Act, he or she must give notice to the California Attorney General who can step in and file the lawsuit instead, or who can require the resident to refrain from filing it altogether.

These fines do not appear to be as hefty as those that can be levied under the GDPR, however the private right of action may spur a new era of California civil litigation.

Disclaimer: This summary is provided for educational and information purposes only and is not legal advice. Any specific questions about these topics should be directed to attorney Arvid von Taube.