Cooley

California Passes Sweeping Consumer Privacy Act

July 3, 2018

On June 27 the California Senate and Assembly unanimously approved the California Consumer Privacy Act of 2018 (CCPA), and Governor Jerry Brown signed it into law the same day. The CCPA was rushed through the legislative process to avoid passage of a more stringent privacy law planned for California's November ballot. Organizations subject to the law must be ready to comply by January 1, 2020.

The law has been characterized as the first "GDPR-like" privacy statute to be enacted in the United States, and includes sweeping changes that will be felt not only in California, but across the nation and the globe. The CCPA will require many organizations that process personal information of California residents to take stock of their privacy and security practices, and update or implement new policies, procedures and controls to address the law.

Significantly, with respect to personal information security breaches, the CCPA provides for a private right of action and the possibility of statutory damages between $100 and $750 per consumer, per incident. In addition, the CCPA deems arbitration clauses and class action waivers as unenforceable and contrary to public policy. The increasingly aggressive California plaintiffs' bar will undoubtedly leverage the law to support a new wave of privacy and data breach class action litigation.

Cooley will soon be supplementing this alert with a detailed FAQ breaking down the CCPA, as well as upcoming presentations and webinars concerning the law and the likely challenges to its enforceability. Some of the law's highlights (the statute is ~10,000 words long and contains numerous drafting errors and typos) are set forth below.

CCPA consumer rights

The Act is intended to provide California consumers with more transparency concerning the use of, and more control over, their personal information. The law defines "consumer" as a natural person who is a California resident, however identified, including by any unique identifier (as such, it appears that consumers would also include an organization's employees who are California residents). The CCPA provides consumers with various "rights", including the right to:

1. know the categories of personal information collected about them, and obtain a copy of their personal information
2. know whether their personal information is sold or disclosed, and to whom;
3. opt out of the sale of their personal information;
4. access and then delete their personal information; and
5. equal service and price (non-discrimination) for individuals that exercise their privacy rights.

Businesses will need to maintain privacy policies describing these rights, as well as implementing procedures to enable consumers to exercise them. The expanded definition of "personal information" in the Act appears intended to pull social media companies, data brokers and online behavioral advertisers under its umbrella, as well as "new" identifiers such as biometric, geolocation and genetic information.

Expanded definition of personal information

The CCPA affects a wide swath of information related to individuals, and will sweep in many types of information (intended and unintended) that have not been previously regulated by privacy laws in the US. "Personal Information" is defined to include information that identifies, relates to, describes, or is capable of being associated with a particular consumer or household. This includes (among other types of personal information)

IP addresses, geolocation data, biometric information, and “unique identifiers” such as device and cookie IDs, Internet activity information like browsing history, commercial information such as products or services purchased or consuming histories or tendencies, and characteristics concerning an individual’s race, color, sex (including pregnancy, childbirth, and related medical conditions), age (40 or older), religion, genetic information, sexual orientation, political affiliation, national origin, disability or citizenship status. Inferences drawn from personal information “to create a profile about a consumer reflecting the consumer’s preferences, characteristics, psychological trends, preferences, predispositions, behavior, attitudes, intelligence, abilities, and aptitudes” are also considered “personal information.”

Privacy policy and procedures

The CCPA mandates new privacy policy disclosures, including a description of a consumer’s rights under the CCPA, disclosures related to a company’s sale of personal information and a summary of an organization’s disclosures of personal information for business purposes. Companies will be required to build out specific procedures to enable individuals to exercise the rights enumerated under the CCPA, including without limitation a webpage entitled “Do Not Sell My Personal Information” that allows the consumer or his or her authorized representation, to opt out of the sale of the consumer’s personal information. Employee training is another requirement – businesses must ensure that all individuals responsible for handling consumer inquiries about their privacy practices or their compliance with the CCPA are informed of the requirements in the CCPA and how to direct consumers to exercise their rights.

Contractual “flow down” provisions and third-party limitations

The CCPA includes a requirement (similar to, but less comprehensive than, the GDPR requirement that controllers must enter into data processing agreements with processors) that businesses that disclose consumers’ personal information to third parties for a business purpose must enter into a written agreement with the third party that prohibits the third party from selling the personal information, retaining, using or disclosing the personal information for any purpose other than for the specific purpose of performing the services specified in the contract, or retaining, using or disclosing the information outside of the direct business relationship between the personal and the business. The CCPA also provides that a third party that purchases personal information cannot resell that personal information unless it provides the consumer with explicit notice and an opportunity to opt out of such resale.

Limitations on consumer waivers and limitations of liability

In a provision that appears targeted at arbitration clauses and class action waivers, the Act also provides that any provision of a contract of any kind that purports to waive or limit a consumer’s rights under the Act, **including any right to a remedy or means of enforcement**, shall be deemed contrary to public policy, void and unenforceable.

Private right of action for personal information breaches; statutory damages

With respect to data breaches, the Act provides a private right of action for individual consumers to recover both actual and statutory damages. Organizations may be liable for personal information breaches if the breach resulted from the failure to maintain reasonable security procedures and practices appropriate to the nature of the affected information. In assessing the appropriate amount of statutory damages, courts are to consider the nature and seriousness of the misconduct, the number of violations, the persistence of the misconduct, the length of time over which the misconduct occurred, the willfulness of the organization’s misconduct, and the organization’s assets, liabilities, and net worth.

To initiate an individual or class action for statutory damages, consumers are required to give companies 30 days written notice of the specific provisions of the CCPA the consumer alleges were violated, and provide

affected organizations the opportunity to cure the violation. In addition, consumers can bring an action only if the Attorney General declines to prosecute within 30 days' notice of a consumer's intent to bring the action. If the affected business does cure within 30 days and provides a written statement confirming the cure, then the affected consumers are precluded from seeking statutory damages. This limitation, however, does not affect an individual's ability to seek actual damages for a violation of the CCPA.

Penalties

The CCPA provides that a business will be in violation of the Act if it fails to cure any alleged violation within 30 days after being notified of alleged noncompliance. Any business, service provider, or other person that violates the CCPA shall be liable for a civil penalty as provided in Section 17206 of the Business and Professions Code in a civil action brought by the Attorney General in the name of the people. Any person, business or service provider that intentionally violates the CCPA may be liable for a civil penalty of up to $7,500 per violation and any civil penalty assessed pursuant to Section 17206. The proceeds of any settlement of such action, shall be allocated 20% to the Consumer Privacy Fund and 80% to the jurisdiction on whose behalf the action leading to the penalty was brought.

Next steps

Like the GDPR, the CCPA will require organizations to take a fresh look at their personal information handling practices, internal policies, procedures and controls, and their external privacy statements and representations. As a first step, we anticipate that companies subject to the CCPA will have to engage in data process flow mapping to inventory their processing activities and identify potential compliance gaps. One silver lining to GDPR may be the existence of data process flow maps that can be utilized in the CCPA context, and the presence of seasoned internal and external practitioners who have been through the exercise before. In addition to supplemental educational pieces, including an upcoming FAQ and one or more webinars breaking down the CCPA, Cooley will be working to develop the tools, forms and know-how to address this law, including developing compliance plans to allow for an efficient risk-based approach to the CCPA.

This content is provided for general informational purposes only, and your access or use of the content does not create an attorney-client relationship between you or your organization and Cooley LLP, Cooley (UK) LLP, or any other affiliated practice or entity (collectively referred to as "Cooley"). By accessing this content, you agree that the information provided does not constitute legal or other professional advice. This content is not a substitute for obtaining legal advice from a qualified attorney licensed in your jurisdiction, and you should not act or refrain from acting based on this content. This content may be changed without notice. It is not guaranteed to be complete, correct or up to date, and it may not reflect the most current legal developments. Prior results do not guarantee a similar outcome. Do not send any confidential information to Cooley, as we do not have any duty to keep any information you provide to us confidential. When advising companies, our attorney-client relationship is with the company, not with any individual. This content may have been generated with the assistance of artificial intelligence (AI) in accordance with our AI Principles, may be considered Attorney Advertising and is subject to our legal notices.

This information is a general description of the law; it is not intended to provide specific legal advice nor is it intended to create an attorney-client relationship with Cooley LLP. Before taking any action on this information you should seek professional counsel.

Copyright © 2023 Cooley LLP, 3175 Hanover Street, Palo Alto, CA 94304; Cooley (UK) LLP, 22 Bishopsgate, London, UK EC2N 4BQ. Permission is granted to make and redistribute, without charge, copies of this entire document provided that such copies are complete and unaltered and identify Cooley LLP as the author. All other rights reserved.