Pepper Hamilton LLP
Attorneys at Law

Latest California Consumer Privacy Act Amendments Impact Business Compliance Initiatives

ALERT | September 16, 2019

Sharon R. Klein | kleins@pepperlaw.com
Alex C. Nisenbaum | nisenbauma@pepperlaw.com
Jeffrey M. Goldman | goldmanj@pepperlaw.com
Taylor Jon Torrence | torrencet@pepperlaw.com

On September 13, the final day of its legislative session, the California Legislature approved five amendments to the California Consumer Privacy Act (CCPA), the state's sweeping new privacy law that takes effect on January 1, 2020. Although the amendments address a number of issues intended to mitigate the compliance burden on businesses, the new exemptions and other modifications and clarifications are limited. The California Legislature also failed to pass a proposed amendment intended to ease compliance burdens for retailers that offer consumer loyalty programs. The amendments:

- exempt, until January 1, 2021, certain employment-related information from all provisions of the CCPA except the CCPA's obligation to inform the consumer of the categories of personal information to be collected and the private civil action provision

- exempt, until January 1, 2021, consumer personal information reflecting a business-to-business communication or transaction from certain notification obligations under the CCPA, but not the CCPA's opt-out right or private civil action provisions

- allow businesses to require authentication that is reasonable in light of the personal information requested under a verifiable consumer request

- modify the requirements for submission of verifiable consumer requests for businesses that operate exclusively online and have a direct relationship with consumers

- require any business that maintains a website to make the website available for submission of verifiable consumer requests

- authorize a business to require a consumer that maintains an account with the business to require that consumer to submit a verifiable consumer request through that account

- make certain clarifying edits to the definition of "personal information"

- limit opt-out and deletion rights of consumers relating to vehicle repair, warranty and recall data.

Although the amendments offer some limited relief to businesses, the California Legislature made clear that any data breach of California resident information, including employee or business-to-business information, will open businesses up to lawsuits under the CCPA's private right of action.

Exemption for Personal Information of Employees

The application of the CCPA to employees' personal information created some of the most complex compliance challenges for businesses. The amendments provide some relief by exempting from most CCPA provisions personal information that is collected by a business about job applicants, employees, owners, directors, officers and contractors,

provided that the information is collected and used by the business solely within the context of that employment or contractor relationship. The amendments similarly exempt personal information used for emergency contact purposes and the administration of employment benefits.

The employee personal information exemption is not absolute. Businesses will still be required to provide employees with information on the categories of personal information the business collects about them, and employees may sue under the CCPA's private right of action in the event of a data breach. The employee personal information exemption is scheduled to sunset on January 1, 2021. As a result, businesses still need to inventory all employee-related data they collect and take other steps to operationalize disclosures of personal information collection practices to employees, for example by adding a CCPA notice to the new hire paperwork of California employees and in the employee handbook. Businesses should also appropriately secure employment-related data to mitigate risk of litigation under the CCPA's private right of action in the event of a data breach.

Business-to-Business Exemption

Because the CCPA broadly defines "consumer" as any California resident, businesses have expressed concerns about the law's application to business-to-business communications. The amendments address this concern by providing a limited exemption for personal information reflecting communications or transactions between a business and a consumer where the consumer is acting as an employee, owner, director, officer or contractor of the business.

This business-to-business related personal information is exempted from the CCPA's notification and deletion requirements as well as requirements to respond to verifiable consumer requests for disclosure. Businesses, however, must still honor requests they receive to opt out of the sale of this business-to-business personal information, and this information is still subject to the CCPA's private right of action. The business-to-business exemption is scheduled to sunset on January 1, 2021.

Because this exemption is limited, businesses will still need to inventory how this data is collected, stored, used and shared by the business in order to operationalize methods to track and restrict the onward transfer of business-to-business personal information and appropriately secure this personal information.

Submitting and Authenticating Verifiable Consumer Requests

The CCPA provides consumers with a number of rights to request information about their data from businesses. Businesses are generally required to respond to verifiable consumer requests for information within 45 days. However, other than requiring that businesses provide at least two methods to submit requests — including a toll-free number and, if the business maintains a website, a website address — the CCPA originally did not provide guidance on how to operationalize submitting consumer requests. Clarification was left to the California Office of the Attorney General, but the Attorney General has yet to enact any regulations.

The amendments provide that a business may require consumer authentication that is reasonable in light of the nature of the personal information requested. This revision provides some standard for evaluating consumers' identities while businesses await more definitive guidance from the California Attorney General. The standard also prohibits businesses from requesting authenticating information that is unduly burdensome for consumers. If a consumer maintains an account with the business, businesses are now specifically allowed to require a consumer to submit a request through that account.

The amendments also make changes to address the mechanics of submitting requests. Businesses are still required to provide two or more designated methods for submitting requests for information, but the amendments clarify that if a business maintains a website, the business must make available a mechanism on that website to submit requests for information. Businesses that operate exclusively online and that have a direct relationship with a consumer are now allowed to provide only an email address for submission of requests for information.

Clarifying Edits to Definition of "Personal Information"

The CCPA's definition of "personal information" is exceptionally broad by design. As originally passed, personal information included any information that "is capable of being associated with" a particular consumer or household, which potentially includes all data held by a business at some point in the data lifecycle. To address this issue, the amendments revise the definition of "personal information" so that data qualifies as personal information when it is "reasonably" capable of being associated with a particular consumer or household. This allows businesses to evaluate whether a particular piece of data is capable of being associated with a consumer or household based on the information and means reasonably available to the business.

The CCPA as originally passed included “deidentified” and “aggregate” data concepts. However, as drafted, the CCPA did not explicitly state this data did not qualify as personal information. The amendments address this issue by revising the law to expressly exclude deidentified and aggregate data from the definition of personal information. Finally, the amendments remove certain restrictions on the use of publicly available data to address commentary that these restrictions may result in First Amendment violations.

Pepper Points

With the 2019 California legislative session concluded, absent regulations or guidance by the California Attorney General or action by California governor Gavin Newsom before signing the amendments, businesses now have a full picture of the CCPA as it will go into effect on January 1, 2020. The latest amendments provide businesses with some helpful relief, but the relief is temporary and limited in scope.

Since the California Legislature left intact the law’s private right of action for California resident personal information, including employee and business-to-business personal information, we can expect plaintiffs will utilize the statutory damage provisions of the CCPA to attempt to avoid proving in detail actual injury for standing in litigation, making lawsuits for data breaches easier to bring and potentially sustain. To prepare for the CCPA, business should:

- continue or begin mapping the California resident-related personal information they collect, including employee and business-to-business related personal information, and use those maps to inform how they will operationalize the CCPA’s various requirements

- conduct security assessments to evaluate the safeguards used by the business and its critical vendors, identify risk and prioritize mitigation efforts — in particular, businesses should make sure all personal information is encrypted while stored and in transit

- prepare and publish public-facing privacy notices and, if applicable, opt-out mechanisms

- update policies and procedures to enable compliance with consumer rights requests

- analyze all third-party service provider contracts and amend them to incorporate the use and disclosure restrictions mandated by the CCPA and add security requirements

- update systems and databases to enable compliance with consumer rights requests, such as opt-out, deletion and disclosure of information collected

- monitor all developments relating to the CCPA, including any regulations and guidance from the California Attorney General.