Not with a Bang but a Whimper: At the Deadline, Minor Amendments to the California Consumer Privacy Act

September 18, 2019

The business community watched eagerly as the California legislature approached a September 13 deadline for amending the California Consumer Privacy Act before it takes effect on January 1, 2020. Many potential amendments were in play, including some that would have made core changes to this major new privacy law. But the only amendments to actually pass were at the margin: human resources files, mergers and acquisition due diligence information concerning employees and officers, and business-to-business communications are now largely out of scope. These amendments generally are business-friendly, but they are not game-changers.

Assuming these amendments are signed by California Governor Gavin Newsom, as is expected, then the shape of the CCPA—and of corporate compliance obligations for the time being—can now be seen with more certainty. Companies subject to the CCPA should take into consideration how these amendments might affect their gap analyses and implementation of any needed policies, procedures, and technical measures. The amendments provide that certain business-friendly exceptions will sunset after a year unless the legislature acts again. Stakeholders also continue to await crucial implementing regulations from the California Attorney General. So it seems likely that all eyes in the privacy community will remain on Sacramento for at least another year.

HUMAN RESOURCES DATA

Pre-amendment, a gray area under the CCPA was that employee data appeared to be in scope under the statute's plain words—even though protection of employees (as opposed to consumers) did not seem to be the legislative purpose. We now have an answer in black and white: For the year 2020, at least, HR data will be out of scope. The amendments exempt personal information that is collected about a California resident in their role as "a job applicant to, an employee of, owner of, director of, officer of, medical staff member of, or contractor" of the covered business. The amendments also exempt emergency contact information for employees as well as personal information necessary for the covered business "to administer benefits" for the employee's dependents or beneficiaries.

Two caveats: (1) covered businesses must still disclose to employees (and to applicants, etc.), at or before the point of collection the categories of personal information they collect; and (2) this exemption does not apply to the CCPA's private right of action for data breaches. Employees, like consumers, will be able to sue, and recover generous statutory damages, if their personal information is compromised.

Practical Takeaway

We have previously suggested that, given the possibility this sort of amendment would pass, businesses might reasonably put HR-related matters at the back of their CCPA compliance queues. It is now clear that, subject to these limited caveats, HR matters can be put out of queue altogether for at least a year. HR information comes back into scope for 2021 and beyond unless the legislature acts again to extend the exemption.

BUSINESS-TO-BUSINESS COMMUNICATIONS AND DUE DILIGENCE INFORMATION

Also for a year, the amendments exempt from much of the CCPA personal information "reflecting a written or verbal communication or a transaction between" a covered business and a consumer who is acting "as an employee, owner, director, officer, or contractor" of another company, where the covered business is engaged in "conducting due diligence regarding, or providing or receiving a product or service" from the other company.

Practical Takeaway

An acquirer that receives consumer-level data relating to the target's employees and officers as part of a proposed deal does not need to apply CCPA protocols to the data room. Let's say you are planning to acquire a software engineering firm, and in due diligence you receive a roster of the target company's employees, officers, and board of directors. You do not need to give the individuals on that roster a CCPA privacy notice, nor do you need to respond to their requests under the CCPA to access their data or to delete their data.

These exemptions do not apply to the provisions concerning consumers' right to opt out of the sale of their data or the private right of action for data breaches.

CONSUMER REPORTS

For consumer reporting agencies, furnishers of consumer report information, and users of consumer reports, activities regulated by the Fair Credit Reporting Act are exempt

from the CCPA. Like the exceptions noted above, the exception for consumer report activities does not apply to the private right of action for data breaches.

DATA BROKER REGISTRATION

The amendments impose a new registration requirement on data brokers. Data brokers are defined as those businesses that "collect and sell to third parties the personal information of a consumer with whom the business does not have a direct relationship." The definition explicitly does not include consumer reporting agencies, financial institutions, or insurance companies. Data brokers are required to register with the Attorney General each year and provide their contact information. The Attorney General is obligated to publish a website to make this information available to the public. The intent of the amendment was to assist consumers in identifying businesses that collect their information and provide them with contact details if the consumer wishes to opt out of the sale of their personal information.

VEHICLE INFORMATION

A narrow exception to the right to opt out of the sale of personal information was created for vehicle information and ownership information shared between a motor vehicle dealer and the vehicle's manufacturer.

ONLINE BUSINESSES

Businesses that operate "exclusively online" and have a "direct relationship with a consumer" will no longer be required to provide consumers with a toll-free number to submit data access requests—an email address alone is sufficient. Other covered entities are obligated to provide at least two methods for consumers to submit data access requests, including, at a minimum, a toll-free telephone number.

"REASONABLE" LIMITS ON PERSONAL INFORMATION

The amendments introduced clarifying changes to the definition of personal information. First, the amendments create a reasonableness requirement with respect to the definition of personal information: in order for information that does not directly identify a consumer to be within scope, that information must "reasonably" be capable

of being associated with a consumer or household. This makes clear that an objective standard will be applied—the mere possibility that information can be linked to an individual is not enough. Second, the amendments make clear that personal information "does not include deidentified or aggregate consumer information." Third, the amendments provide additional clarity as to what qualifies as "publicly available information." Publicly available information is exempt from the definition of personal information and is "information lawfully made available from federal, state, or local government records."

DATA BREACH NOTIFICATION EXPANDED

Related to, but separate from, the CCPA amendments, the legislature also passed a bill that broadened the definition of personal information in the context of data breaches. The definition now includes tax identification numbers, passport numbers, military identification numbers, and other unique identification numbers issued on a government document as well as biometric data.

BIGGER AND BOLDER AMENDMENTS FAILED

Amendments were considered, but not passed, that would have exempted personal information collected "as part of loyalty, rewards, premium features, discounts or club card programs" and personal information disclosed to third parties for the sole purpose of detecting security incidents. An effort led by Google and others to carve out targeted internet advertising did not make it through either. Earlier this year, a bill that was supported by California's Attorney General that would have broadened a consumer's private right of action was withdrawn. As a result, the private right of action applies to data breaches but not to any missteps in day-to-day CCPA compliance. For example, a failure to tag data as "do not sell" when a consumer so requests could draw enforcement action from the California AG, but not from the plaintiffs' bar.

* * *

Our Cybersecurity and Data Privacy Team would be pleased to discuss these issues with you. Please do not hesitate to contact us with any questions.

WASHINGTON, D.C.

Jeffrey P. Cunard
jpcunard@debevoise.com

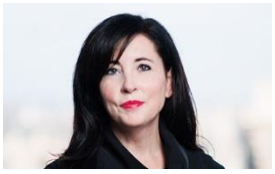
Luke Dembosky
ldembosky@debevoise.com

NEW YORK

Jeremy Feigelson
jfeigelson@debevoise.com

Jane Shvets
jshvets@debevoise.com

Jeremy C. Beutler
jcbeutler@debevoise.com



Maura Kathleen Monaghan
mkmonaghan@debevoise.com

Jim Pastore
jjpastore@debevoise.com

Emily Rebecca Hush
erhush@debevoise.com