Amendments to the California Consumer Privacy Act of 2018

September 26, 2018

California Governor Jerry Brown has just signed into law a set of amendments to the California Consumer Privacy Act (the "Act"). As we observed in our prior Client Update, the Act grants broad new privacy rights to California consumers and imposes new obligations on businesses that collect or use consumers' personal data. While the Act remains the biggest and boldest expansion of U.S. privacy law in years, the amendments provide exemptions for specified entities and information. These exemptions narrow the Act's application in a way that should significantly benefit business, particularly healthcare and financial services companies.

Debevoise & Plimpton

What are the new exemptions? The amendments provide that the Act does not apply either to "a covered entity governed by the privacy, security and breach notification rules" of the federal Health Insurance Portability and Accountability Act ("HIPAA"), or to "a provider of health care" governed by California's Confidentiality of Medical Information Act. These exemptions apply to "the extent the provider or covered entity maintains patient information in the same manner as medical information or protected health information" governed by HIPAA's privacy, security and breach notification rules.

In addition to these *entity* exemptions, the amendments exempt certain *types* of information:

- "[P]rotected health information" collected by "a covered entity or business associate" governed by HIPAA's privacy, security and breach notification rules as well as "medical information governed by [California's] Confidentiality of Medical Information Act." This is an expansion of the exemption under the original text of the Act, which was limited to protected health information collected by HIPAA-covered entities only.

- "Information collected as part of a clinical trial subject to the Federal Policy for the Protection of Human Subjects, also known as the 'Common Rule.'"

- "[P]ersonal information collected, processed, sold or disclosed pursuant to" the Gramm-Leach-Bliley Act ("GLBA") and its implementing regulations and

information governed by the California Financial Information Privacy Act. The prior exemption limited the Act's application only to the extent it conflicted with GLBA.

- "[P]ersonal information collected, processed, sold, or disclosed pursuant to the Driver's Privacy Protection Act of 1994." The prior exemption applied only to situations in which the Act conflicted with the Driver's Privacy Protection Act.

It appears that a company may be covered by these exemptions for some purposes and not others—that is, it may collect and use certain information in a way that is exempt, and other information in a way that is still subject to the Act. For example, not all information handled by a financial institution is necessarily handled "pursuant" to GLBA.

Notably, the exemptions for information covered by GLBA, the California Financial Information Privacy Act, and the Driver's Privacy Protection Act apply to many of the Act's provisions concerning disclosure, sale and deletion of consumer information but do not extend to the Act's private right of action for consumers. Unlike the bulk of the Act, which deals with the collection and usage of personal data in the ordinary course, the private right of action is directed to data breaches: a California consumer whose data is exposed in a breach can recover statutory damages ranging from $100 to $750 per California consumer per incident.

After the amendments, the Act's definition of "personal information" for data breach purposes remains narrower than for day-to-day data handling purposes: the more traditional and limited definition of personal information under California's preexisting data breach notification law still applies. Under the amendments, a consumer may still bring an action for a data breach involving information covered by GLBA, the California Financial Information Privacy Act and the Driver's Privacy Protection Act.

Are there any changes to the effective date? The amendments do not change the Act's overall effective date of January 1, 2020. The amendments do extend the deadline for the Attorney General to "adopt regulations to further the purposes of" the Act by six months to July 1, 2020. The Attorney General may not bring an enforcement action under the Act until the earlier of (1) six months after the Attorney General publishes the final regulations or (2) July 1, 2020.

The provision of the Act that preempts local laws takes effect immediately. This appears to be intended to prevent local governments from enacting conflicting requirements between now and 2020.

How do the amendments change enforcement? The amendments remove the requirement that consumers notify the Attorney General prior to bringing an action for

a data breach. Relatedly, the Attorney General no longer has a right to bar consumer plaintiffs from bringing suit, as it did under the prior version of the Act.

The amendments also provide that the Attorney General may seek injunctive relief in addition to civil penalties.

What other changes should businesses be aware of? The amendments supplement the examples of "personal information" set out in the Act. Each example is considered "personal information" if it "identifies, relates to, describes, is capable of being associated with, or could be reasonably linked, directly or indirectly, with a particular consumer or household." This largely continues the extremely broad definition of "personal information" in the original Act, while the focus on "a particular consumer or household" perhaps narrows a bit how it might be interpreted. In addition, the amendments clarify that the Attorney General may seek civil penalties of up to $7,500 per intentional violation and $2,500 for other violations.

How do the amendments change how businesses should prepare? Our earlier Client Update suggested some steps businesses might consider before the Act takes effect. Those suggestions, beginning with a diligence exercise to determine the scope of covered data being held by a company, still hold after the amendments. In addition, businesses should evaluate the new exemptions to determine what relief they might bring. Keep in mind that, as noted above, under the amendments an entity may be partly in and partly out—that is, exempt as to some of the data it collects and holds, but not as to all data. In light of the amendments, the internal diligence process might focus in part on sorting data into exempt and nonexempt buckets.

* * *

Our Cybersecurity and Data Privacy Team will continue to provide updates on the Act. We would be pleased to discuss these issues with you.

NEW YORK

Jeremy Feigelson
jfeigelson@debevoise.com

Maura Kathleen Monaghan
mkmonaghan@debevoise.com

Jim Pastore
jjpastore@debevoise.com

Jeremy C. Beutler
jcbeutler@debevoise.com

WASHINGTON, D.C.

Luke Dembosky
ldembosky@debevoise.com

LONDON

Jane Shvets
jshvets@debevoise.com