NOW + NEXT

JULY 2, 2018

California's own GDPR? Big win for consumer privacy advocates could spell trouble for companies that sell personal data

By Karina Puttieva and Jenny Holmes

Just a month after the European Union's notoriously strict General Data Protection Regulation (GDPR) went into effect, California followed suit with a landmark law of its own: the California Consumer Privacy Act of 2018.

Authored by democrats Senator Bob Hertzberg and Assemblyman Ed Chau, AB 375 passed unanimously in both chambers of the California Legislature on June 28. Mere hours later, Governor Jerry Brown signed the bill into law.

The law's opponents—including major tech companies like Facebook, as well as the California Chamber of Commerce, the National Retail Federation and the Association of National Advertisers—nonetheless urged its passage. The opponents were understandably anxious about the more expansive ballot initiative that San Francisco real estate developer Alastair Mactaggart had qualified for the November ballot. Unlike ballot initiatives, laws passed through the legislature are easier to amend. And the law's opponents already put together a list of changes they want to make to the statute before it goes into effect in 2020. Mactaggart, who had agreed to withdraw his initiative from the ballot if the governor signed AB 375, kept his word and pulled the initiative later on June 28.

What does the new law do?

Set to go live on January 1, 2020, the law protects California consumers and applies to all businesses that meet one or more of the following thresholds:

- have annual gross revenues in excess of $25 million;
- annually buy, sell or share personal information of 50,000 or more consumers, households or devices; or
- derive 50% or more of their annual revenues from selling consumers' personal information.

Much like the GDPR, the law drastically expands the definition of "personal information" to include things like

- unique personal identifiers, such as persistent cookies, user alias and mobile ad identifiers
- IP addresses
- browsing and search history
- geolocation data
- inferences drawn from personal information about consumer's preferences, characteristics, behavior, attitudes and the like.

Under the new law businesses must, upon request, disclose to California consumers

- **What** personal information is being collected about them
- **Where** the business gets that personal information from
- **Why** the personal information is collected
- **What** category of third parties the personal information is shared with
- **Whether** the business sells their personal information and to whom

Businesses must also comply with a California consumer's request to

- **Stop selling** their personal information
- **Delete** their personal information

Businesses are banned from

- Selling personal information about children under 13, unless there is parental consent
- Selling personal information about children under 16, unless they affirmatively opt in

Businesses cannot discriminate against consumers for exercising their rights, such as by charging them higher fees or delivering lower quality service or products. But they can still offer financial incentives for collection of personal information.

Consumers can sue businesses for data breaches of unencrypted, unredacted information, with damages of at least $100 and up to $750 per consumer per incident or actual damages, if they are higher. The California attorney general is allowed to step in to take the case, and businesses must be given a chance to "cure" the violations—but it's unclear how a data breach can be cured after the fact.

What this means for businesses

Hailed as the strictest data privacy law in the United States, the California Consumer Privacy Act is a game-changer. And privacy experts predict that the law will have ramifications well beyond California, given the hassle and expense of building state-by-state consumer experiences.

Businesses who went through the painful process of GDPR compliance likely have little to worry about since the California law is far less strict.

The rest, however, will have to keep a close eye on any amendments that will flesh out the law over the next year and a half. Now would be a good time to undertake a data audit and determine

- what kind of information your business collects and shares about consumers—including data we don't traditionally think of as "personal"—how your business collects it, and where that data goes
- whether you have the technical capabilities to respond to consumers' requests to delete their information
- whether you have the technical capabilities to separate a consumer's data from the data that is being sold, if a consumer requests that your business no longer sell their data
- what you are doing to protect consumer information, especially because the law includes a private right of action for data breaches and sets minimum statutory damages.

If you have any questions about your business's data privacy compliance with the existing regulatory structure and how the GDPR or California's new law may affect you, please contact your regular Nixon Peabody attorney or:

- Karina Puttieva at **kputtieva@nixonpeabody.com** or 213-629-6091
- Jenny L. Holmes at **jholmes@nixonpeabody.com** or 585-263-1494
- Jason P. Gonzalez at **jgonzalez@nixonpeabody.com** or 213-629-6019
- Steven M. Richard at **srichard@nixonpeabody.com** or 401-454-1020