THOMSON REUTERS

Westlaw®

A new privacy and data control framework in California

By Jeffrey Poston, Esq., Paul Rosen, Esq., Maarten Stassen, Esq., and Josh Thomas Foust, Esq., *Crowell & Moring**

AUGUST 14, 2018

The California legislature passed one of the nation's strictest data privacy rules on June 28, marking a watershed moment in U.S. data privacy reform.

The California Consumer Privacy Act of 2018 (AB-375)[1] gives Californians several specific rights to control the movement of their personal information, including the right to know what is being collected about them and what is being sold and re-disclosed, and the right to prevent the sale of their personal data.

The passage of this law will substantially impact the data use policies of major technology companies and retailers, and could serve as a catalyst for federal data privacy legislation.

It also creates a private right of action for data breaches that result in disclosure of personal information, without any requirement of proof of harm. This could lead to a flood of new class actions arising out of data breaches.

Unless the Act is changed by subsequent legislation or a new successful ballot initiative, the law will go into effect on January 1, 2020.

WHAT DOES THE LAW DO?

The California Consumer Privacy Act:

- Directs companies to make disclosures about the information they collect from consumers and their business purposes for the data collection.
- Grants consumers the right to request deletion of their personal information through a "verified request" and to opt out entirely from the sale of their personal information.
- Prohibits companies from discriminating against consumers for exercising any of these rights. However, the law does allow companies to offer financial incentives for collection of personal information.
- Prevents businesses from selling the personal data of online consumers under the age of 16.
- Makes it easier for consumers to sue companies following a data breach.

The legislation adopts an expansive definition of "personal information," including identifiers such as IP addresses, internet or other electronic network activity information such as browsing history and search history, geolocation data, and any inferences drawn from these data to create a profile about a consumer's preferences, behavior, or characteristics.

HEADING OFF A MORE SWEEPING BALLOT INITIATIVE

This legislation was fast-tracked to preempt a ballot initiative backed by Californians for Consumer Privacy, a coalition of consumer protection and advocacy organizations, which was picking up support ahead of a November vote (the ballot initiative has since been withdrawn).[2]

There are a few substantive policy differences between the two. For example, under the ballot initiative, companies would not be able to deny a consumer service if they opt out of certain data uses.

The AB-375 legislation does allow companies to offer different tiers of service, as long as the difference in tiers is *reasonably related to the value provided to the consumer* by the consumer's data. The precise meaning of these terms will be hashed out in court.

The new legislation's private right of action authorizing consumers to sue is also significantly more restrictive than the expansive mechanism proposed in the ballot initiative, which many feared would fuel a surge in class-action litigation.

The ballot initiative would have allowed consumers to sue not only for violations of the law's requirements, but also for data breaches involving the consumer's information, and provided statutory damages of $1,000 to $3,000 per violation.

The ballot initiative also expressly provided that any violation of the statute would constitute an "injury in fact" — an evident attempt to ground standing in federal courts under *Spokeo, Inc. v. Robins*.[3]

As explained further below, the new legislation, by contrast, limits the statutory damages available for violations, while also giving companies the right to cure alleged violations before being hauled into court.

Unlike the ballot initiative, the law does not expressly provide that violations automatically constitute "injuries in fact," which benefits companies seeking to argue that "harmless" or "technical"

Thomson Reuters is a commercial publisher of content that is general and educational in nature, may not reflect all recent legal developments and may not apply to the specific facts and circumstances of individual transactions and cases. Users should consult with qualified legal counsel before acting on any information published by Thomson Reuters online or in print. Thomson Reuters, its affiliates and their editorial staff are not a law firm, do not represent or advise clients in any matter and are not bound by the professional responsibilities and duties of a legal practitioner. Nothing in this publication should be construed as legal advice or creating an attorney-client relationship. The views expressed in this publication by any contributor are not necessarily those of the publisher.

the answer company™
THOMSON REUTERS®

violations should not create standing in federal court to enforce the law.

IMPLEMENTATION AND ENFORCEMENT

Companies will be required to clearly post a link titled "Do Not Sell My Personal Information" that allows a consumer to opt out of the sale of the consumer's personal information.

Separate or additional homepages for California-based residents are permissible as long as the company takes reasonable steps to redirect California residents to that specific page.

Upon receiving a verifiable request, companies must deliver any collected "categories and specific pieces of personal health information" to the consumer within 45 days.

As mentioned above, the law creates a private right of action for consumers to sue based on the unauthorized access, disclosure, or theft of their non-encrypted or non-redacted information "as a result of the business' violation of the duty to implement and maintain reasonable security procedures and practices appropriate to the nature of the information to protect the personal information."

The new legislation provides for statutory damages of $100 to $750 per violation, unless the consumer suffered "actual damages" exceeding that limit. Importantly, "actual damages" are not a prerequisite to bringing suit.

Before filing a class action or individual suit for these statutory damages, the consumer must provide the company with 30 days written notice of the specific violations alleged. If the business "actually cures" the alleged violations within 30 days, the consumer is barred from bringing suit.

Within 30 days of actually filing an action, the consumer must notify the California Attorney General.

The legislation essentially gives the Attorney General a "first right of refusal": the consumer may only proceed with the suit if, within 30 days, the Attorney General declines to prosecute the action.

The law does not contain a private right of action for violation of its restrictive opt-out provisions, but it does create a new private action for data breaches resulting in disclosure of personal information. In such cases, aggrieved consumers can sue even without proof of harm.

This potentially expands considerably the potential class action risk for data breaches in California. Previously, under California's Data Breach Notification Law, companies had a duty to notify California residents who had become victims of data breaches, but did not attach potential damages to the failure to prevent such breaches by third parties.[4]

That said, companies will have potential defenses against liability under the new law based on the requirement that the breach or theft of consumers' information be "the result of" the company's failure to implement "reasonable security procedures" that are proportionate to the "nature of the information" at issue.

In addition to enforcement duties, the Attorney General is also directed to create additional regulations implementing the legislation, kicking off what will undoubtedly be a long process of public input from both consumer groups and industry.

ENHANCED PRIVACY PROTECTIONS AROUND THE GLOBE

The legislation bears some similarities to the European Union's General Data Protection Regulation (GDPR), particularly the transparency requirements, the right to request deletion, and a strict data breach regime.

Considerations around overlap with the Asia-Pacific Economic Cooperation (APEC) Privacy Framework and the APEC Cross-Border Privacy Rules (CBPR) system will also be important. Companies will be looking for assurances that they can move data across borders both within the US, across the Asia-Pacific region and with the E.U.

WHAT'S NEXT?

Industry groups are already mobilizing on efforts to reform the legislation, which many see as overly restrictive and difficult to implement for internet economy business models.

TechNet, a national coalition that has been fighting against the ballot initiative for some time, stated that "even [the legislation's] authors have acknowledged it is far from perfect and will need revisions in the months ahead as its consequences and workability are better understood."

Over the next two years before the law goes into effect, we'll likely see companies engaging in heightened state, federal and international lobbying efforts, working out the overlaps and differences between this California legislation and other privacy regimes like GDPR and the APEC CBPRs and rapidly moving to revise their privacy policies and practices.

NOTES

[1] The full text of the bill is available online at https://bit.ly/2z68PCO.

[2] California Secretary of State, Proponents Withdraw Initiative to Establish New Consumer Privacy Rights; Expand Liability for Consumer Data Breaches, June 28, 2018, https://bit.ly/2KICC5o.

[3] 136 S. Ct. 1540 (May 16, 2016).

[4] Cal. Civ. Code § 1798.82.

This article first appeared on Practitioner Insights Commentaries on August 14, 2018.

* © 2018 Jeffrey Poston, Esq., Paul Rosen, Esq., Maarten Stassen, Esq., and Josh Thomas Foust, Esq., Crowell & Moring

ABOUT THE AUTHORS




(L-R) **Jeff Poston** is a partner with **Crowell & Moring** in Washington, where he serves as a member of the litigation group and co-chair of the privacy and cybersecurity group. **Paul Rosen**, a former federal prosecutor and chief of staff at the Homeland Security Department, is a partner in the firm's white collar and regulatory enforcement group, privacy and cybersecurity group, and government contracts groups. He works out of the Los Angeles and Washington offices. **Maarten Stassen** is a senior counsel in Crowell & Moring's Brussels office, where he is a member of the privacy and cybersecurity group. **Josh Thomas Foust** is a counsel in the firm's San Francisco office and is a member of the litigation group and advertising and product risk management group. This expert analysis was first published June 29 on the firm's website. Republished with permission.

Thomson Reuters develops and delivers intelligent information and solutions for professionals, connecting and empowering global markets. We enable professionals to make the decisions that matter most, all powered by the world's most trusted news organization.

This publication was created to provide you with accurate and authoritative information concerning the subject matter covered, however it may not necessarily have been prepared by persons licensed to practice law in a particular jurisdiction. The publisher is not engaged in rendering legal or other professional advice, and this publication is not a substitute for the advice of an attorney. If you require legal or other expert advice, you should seek the services of a competent attorney or other professional. For subscription information, please visit legalsolutions.thomsonreuters.com.