Privacy Law Goes Big: California's New Consumer Privacy Act

July 3, 2018

California has just enacted the biggest and boldest expansion of U.S. privacy law in years: the California Consumer Privacy Act. It was passed by unanimous vote of the legislature on June 28, 2018 and signed the same day by Governor Jerry Brown. The Act moved through the legislative process from start to finish in just a few days. As a result, 18 months from now, California consumers will have broad new rights to access and erase their personal information and to prevent its sale. Covered businesses will have significant new obligations to disclose their privacy practices, limit their use of personal data, and respond to consumers seeking to enforce their new rights. Consumers also will have a new right to sue after certain data breaches.

Debevoise & Plimpton

How Did This Happen so Fast?

Credit the heightened privacy awareness that followed Cambridge Analytica. A referendum proposing even tougher privacy standards than the Act's was set to be put before California voters this fall. The legislature thus moved quickly to put its own bill together. The business community basically decided to stand back and let the legislature act—passing a bill that business doesn't love in order to preempt a referendum that it loved even less.

Does the Act Apply to My Organization?

The Act applies to for-profit businesses that meet one of the following three criteria: (1) have $25 million in annual revenue; (2) transact with more than 50,000 California residents' data annually; or (3) derive 50 percent or more of annual revenue from selling the data of California residents. The revenue threshold is global, not California-specific, and will be increased every two years based on the U.S. Consumer Price Index.

$25 million in revenue and 50,000 consumers are not big numbers in the scheme of things. The legislative intention is clearly to cover virtually all substantial national companies. International, too: there is no exemption for companies based overseas. Note that $25 million in global revenue is all it takes for a for-profit organization to be covered—even if it does not have 50,000 customers in California. Constitutional

standards of personal jurisdiction of course would still have to be met for a non-California-based business to be covered.

When Does the Act Take Effect?

January 1, 2020.

What Kind of Data Is Covered by the Act?

"Personal information" is defined very broadly. Any data that "identifies, relates to, describes, is capable of being associated with, or could reasonably be linked, directly or indirectly, with a particular consumer or household" is covered. Think of it as a "breadcrumbs" definition—whatever might lead back to the consumer is covered. The Act's definition specifically references, for example, Internet activity, geolocation data, employment-related information, consumer purchase histories, biometric data and even "olfactory" information. ("Olfactory" is undefined - one thing among many in the Act that awaits possible clarification by the California legislature or by the state attorney general, who is empowered to "solicit broad public participation to adopt regulations to further the purposes" of the Act.) Going even further, the Act also defines as "personal information" any "inferences" that could be drawn from any of the listed categories of personal information to create a profile.

What Must Covered Businesses Do Under the Act?

Among other things:

- Disclose to consumers how their personal information is used prior to, or at the time of, collection.
- Inform consumers that they can opt out of the sale of their personal information and that they have a right to have their information deleted.
- Within 45 days of a consumer request:
    - provide details on the consumer's personal information held by the company;
    - disclose what categories of third parties (if any) the customer's personal information has been transferred to;
    - disclose the personal information's source;
    - cease selling, or delete entirely (with some exceptions), the consumer's personal information;

- Provide a clear and conspicuous link on their California-facing homepage titled "Do Not Sell My Personal Information," linking to a location where a user can opt out of the sale of her personal information;

- Provide consumers with at least two methods of contacting the business for information disclosures, including a toll-free number and a website, and

- Train any employee who might receive a consumer's request about his rights under the Act.

Do Businesses Have Any New Rights or Opportunities Under the Act?

For consumers who opt out of the sale of their personal information, the company can impose a charge—but the charge may not exceed the lost revenue from the consumer's choice. A business can also exclude vendors from falling within the definition of third party under the Act by securing contractual commitments from the vendor not to sell the information transferred to them, not to disclose the information outside the business relationship, and to only use the information for the specific purpose for which the personal information is provided to the vendor.

What About Children?

Consumers under 13 continue to be protected primarily by the federal Children's Online Privacy Protection Act. The Act adds new protections as well. Sale of consumer data for consumers under 13 can only take place on an "opt-in" basis, i.e., if the child's parent or guardian has affirmatively consented. The same is true for consumers between 13 and 16, except that those consumers can give their own consent.

What About Data Breaches?

California consumers whose data is exposed in a breach now can recover statutory damages ranging from $100 to $750 per California consumer per incident. The Act does contain safe harbors for companies that experience a breach, including a 30-day cure period (likely only applicable to small personal information incidents). There is a requirement that, prior to filing suit, plaintiffs notify the California Attorney General, who has a right to bar the consumer plaintiffs from bringing suit. There is no attorneys' fees provision.

Notably, the Act's broad new definition of "personal information" is *not* exported to the data breach arena. The new private right of action kicks in only when the pre-existing breach notification law's narrower, more traditional definition of personal information is met. That definition covers a person's "first name or first initial and his or her last name in combination with" data elements such as a financial account number (plus any

required password), SSN, driver's license number, or username or email address (plus password). In short, disclosure of "breadcrumbs" is not defined as a breach and triggers no right to sue.

Who Can Enforce the Act?

The California Attorney General may bring civil actions to fine companies that are found noncompliant. There is no consumer private right of action other than for data breaches. The Act says that nothing in it "shall be interpreted to serve as the basis for a private right of action under any other law." This appears to mean no suits for violations of the Act will be permitted under California's general consumer protection statute, Section 17200 of the Business and Professions Code. Unlike the comparable laws of most other states, Section 17200 allows suits for acts that are not just "unfair" or "deceptive" but "unlawful." This can allow for Section 17200 to serve as a back door to a private right of action under other laws that do not themselves allow one. The legislature appears to have closed that back door here.

How Does the Act Compare to the GDPR?

The Act is similar, but not identical, to the GDPR:

The Act	The GDPR
Covers only for-profit entities meeting one of three threshold criteria, based on revenue or volume of information collected. Doing business with 50,000 or more Californians is one of the three possible grounds for coverage, but is not required.	Covers processing of personal data by all entities (for-profit or nonprofit) with an "establishment" in the EU, or entities outside the EU who offer goods and services to individuals in the EU (a/k/a monitoring or targeting EU data subjects from outside the EU).
Defines "personal information" broadly to include broad categories of data that directly or indirectly identifies a person. Publicly available information is excluded.	Defines "personal data" broadly to include broad categories of data that directly or indirectly identifies a person. Publicly available information is included.
Requires third-party vendor agreements to prohibit vendors from retaining, using or disclosing personal information for any purpose besides the services to be performed.	Requires third-party vendor agreements to contain a standard set of commitments to compliance with GDPR standards.
Grants consumers the right to be informed of, to access and (in more limited circumstances) to obtain deletion of their personal information.	Grants consumers the right to be informed of, to access, to correct, (in more limited circumstances) to delete, to restrict processing of and to obtain a portable copy

	of their personal data.
Grants consumers the right to opt out of the sale of their personal information.	Requires entities to have a lawful basis for processing information if not seeking consumer consent.

Is the Act Likely to Change Before It Goes into Effect in 2020?

Lobbying efforts to make the Act more business-friendly will surely continue. The California legislature has the right to amend the Act. It would not have had the right to amend a law passed by referendum. This appears to be why the business community elected not to fight the bill's rush to passage.

Is the Act Effectively a New National Standard?

Not directly. On its face, the Act only applies directly to how your organization treats California consumers.

Very possibly, the Act may set a new standard in a practical sense. *First*, other states have been known to follow California's lead on privacy law. Nobody should be surprised if other state legislatures now pass similar bills. *Second*, companies will face a tough choice. They can voluntarily apply the burdensome terms of the Act to all their consumers regardless of state of residence or create a whole set of policies, procedures and platforms just for handling the personal information of Californians. The all-consumers approach may prove operationally easier for many companies.

What Should Businesses Do to Prepare?

Businesses across the country and the globe should start by determining if they fall within the scope of the Act at all. For the many that do, the good news is you have 18 months to get ready:

- Evaluate the pros and cons of complying just as to California consumers vs. complying as to all consumers. Pick an approach.
- Consider the technical measures and company policies that will be necessary. Start drafting.
- Then implement and test your procedures for responding to consumer requests and meeting corporate obligations. Companies may want to run simulation drills a la tabletop exercises in cybersecurity.
- Robust data mapping will help ensure effective response to data access and deletion requests. You can't provide it or purge it if you don't know where it is.

- Consider whether there are lobbying efforts, perhaps being conducted by trade associations in your industry, that you would like to join in order to seek legislative reform of the Act – or the issuance of clarifying regulations – before the Act takes effect.

* * *

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

NEW YORK

Jeremy Feigelson
jfeigelson@debevoise.com

Maura Kathleen Monaghan
mkmonaghan@debevoise.com

Jim Pastore
jjpastore@debevoise.com

Will Bucher
wwbucher@debevoise.com

Julia Shu
lshu@debevoise.com

WASHINGTON, D.C.

Luke Dembosky
ldembosky@debevoise.com

LONDON

Jane Shvets
jshvets@debevoise.com