CORPORATE COUNSEL
An ALM Website
corpcounsel.com | July 16, 2018

Understanding California's Game-Changing Data Protection Law

By Emily Tabatabai, Antony Kim and Jennifer Martin

For any company that has assets in California or handles Californians' personal information – regardless of the company's location -- California's new Consumer Privacy Act of 2018 will likely have a significant impact on core business operations. That's true whether your business is based in New York, Europe or Asia. Gov. Jerry Brown signed off on this sweeping legislation on June 28 -- just before the deadline to prevent an even more restrictive initiative from being locked into the November California ballot.

The Act borrows heavily from a broad range of existing, global privacy and consumer protection rules and regulations. It is a privacy melting pot, expanding on existing California rules, including the Online Privacy Protection Act (CalOPPA), Shine the Light, and so-called Internet Eraser law, and flavored heavily with EU General Data Protection Regulation (GDPR) style data-ownership and control rights, hints of the Illinois Biometric Privacy Act (BIPA), Vermont's recently passed data broker law, and the Children's Online Privacy Protection Act (COPPA), and nods to various industry best-practice guidance (e.g., FTC's Data Broker Report; DAA self-regulatory guidelines for online behavioral advertising).

Emily Tabatabai, Antony Kim and Jennifer Martin

While the January 2020 compliance deadline provides some possibility for changes or clarifications to the Act's most onerous provisions, companies are well advised to assess readiness, identify gaps, prioritize and remediate well in advance of the effective date.

> California's new Consumer Privacy Act of 2018 will likely have a significant impact on core business operations.. whether your business is based in New York, Europe or Asia.

The Consumer Privacy Act Of 2018: What Businesses Need to Know

1. The Act applies to most companies with California-based assets or customers. As a threshold matter, the Act applies to any "business" that (i) does business in California, (ii) collects California consumers'"personal information" (which includes persistent identifiers), and (iii) satisfies one or more of the following thresholds: (A) annual gross revenues over $25 million; (B) buys, receives, sells, or shares (for commercial purposes) the personal information of 50,000 or more Californian consumers, households or devices; or (C) derives 50% or more of its

revenues from selling consumers' personal information.

Thus, even a small company with less than $25 million in revenues could still be subject to the Act if it has at least 50,000 unique California visitors annually to its website and makes money by or otherwise engages in interest-based advertising. Moreover, the definition of "business" is not limited to online enterprises and could be applied to exclusively brick-and-mortar establishments that do business in California.

2. The Act significantly expands the definition of "personal information" to cover almost any consumer-related data that a company collects or maintains. In addition to the usual suspects (e.g., name, Social Security Number, biometric identifiers, geolocation information, etc.), the definition of "personal information" also includes:

- **Tracking data and unique identifiers,** such as an IP address, cookies, beacons, pixel tags, mobile ad identifiers and similar technology, customer numbers, unique pseudonyms, "probabilistic identifiers" that can be used to identify a particular consumer or device, and other persistent identifiers that can be used to recognize a consumer, family or device over time and across different services.
- **Behavioral and profiling data,** including (i) browsing history, search history, and information regarding a consumer's interactions with a website, application or advertisement," (ii) purchasing history, including products or services that were obtained, purchased or considered, or purchasing tendencies, and (iii) inferences drawn from the foregoing to create a profile reflecting the consumer's preferences, characteristics, psychological trends, predispositions and attitudes.
- **Professional and personal background data,** including "professional or employment-related information," as well as "education information" that is not considered publicly available personally identifiable information under the Family Educational Rights and Privacy Act (FERPA), and "characteristics of protected classifications under California or federal law."
- **Other sensory data,** including "audio, electronic, visual, thermal, olfactory or similar information."

The extensive list of inclusions and exceptions to "personal information" raises significant questions as to how the Act will address de-identified or anonymized data. The Act proclaims that it shall not restrict a business's ability to collect, use, retain or disclose de-identified or aggregated consumer data, yet the definition of personal information includes data that "is capable of being associated with, or could reasonably be linked, directly or indirectly, with a particular consumer or household."

Given the increasing availability of technology capable of re-identifying data by combining sets from various sources, companies should exercise caution when pursuing data anonymization or de-identification strategies.

3. The Act requires consent from children age 13-16 to sell personal information. The Act requires a business to obtain a parent's or guardian's "affirmative authorization" to sell or disclose personal information of a child under 13 to a third-party for non-business purposes, consistent with the U.S. COPPA law. The Act also prohibits a business from selling personal information of a child between ages 13-16 absent affirmative authorization from the child (called the "right to opt-in"). Unfortunately, no guidance is provided as to how underage users should be identified or how opt-in should be achieved. In practice, this could require an affirmative opt-in consent to engage third-party tracking technology on a website when the business has actual knowledge that children ages 13-16 use the website (or has willfully disregarded such knowledge). Because teenagers are so active online and are a desirable demographic for many commercial websites and applications, this requirement could create a significant burden for businesses operating in California.

4. The Act establishes first-in-kind data ownership and control rights. Building off California's existing Shine the Light law (and similar to GDPR), the Act provides consumers with substantial rights to data transparency, access, portability, deletion, and choice over data use and sales to third parties.

In brief, a California consumer may request that a business:

Disclose the types of personal information it collects and shares with third

parties. In an apparent effort to address the opacity of third-party data sales, the Act specifies the following:

- Businesses that collect personal information must disclose: a list of the categories and specific pieces of personal information collected from the consumer.
- Businesses that collect information about a consumer from a source other than the consumer, must disclose: (a) the categories and specific pieces of personal information the business has collected about the consumer, (b) the sources of such information, (c) the business or commercial purpose for collecting or selling the information, and (d) the categories or third parties to whom the business has shared the personal information.
- Businesses that sell consumer information to third parties (for monetary or non-monetary consideration) or disclose consumer information to a third-party for a business purposes must disclose: (a) the categories of personal information collected about the consumer; (b) the categories of personal information sold and the categories of third parties to whom each category of personal information was sold, and (c) the categories of personal information that the business disclosed about the consumer for a business purpose.

Provide access to the personal information collected by the business, in a format that allows the data to be transmitted to another entity (similar to the GDPR requirement of "data portability").

Delete personal information about the consumer that the business has collected from the consumer, and instruct its service providers to delete the consumer's information from their records, subject to certain enumerated exceptions.

- **Honor opt-out** requests from consumers to prevent future data sales to third parties (which does not include service providers). Once opted-out, the consumer must provide express authorization for any future sale of her personal information, and the business may not request re-authorization for a minimum of 12 months.

5. The Act requires development of consumer-facing compliance mechanisms and related protocols. Even businesses that have updated their data management policies and procedures to comply with GDPR may need to design and implement additional mechanisms to comply with the Act.

Businesses must provide two mechanisms or methods for consumers to submit requests for information disclosures, including, at a minimum, a toll-free telephone number and a website address.

- Businesses must provide any consumer-requested disclosures within 45 days of the consumer's request, not more than twice per year, and only if the company is able to "reasonably verify" the identity of the consumer making the request. The California Attorney General is empowered to promulgate regulations to define consumer-identity verification protocols or resources.
- Businesses must add a clear and conspicuous link on their homepage titled "Do Not Sell My Personal Information," which takes consumers to an opt-out tool that prevents their personal information from being sold or disclosed to third parties for non-business purposes. Unlike CAN-SPAM, the Act does not limit the number of links a consumer must click-through to opt-out, though we expect that the California Attorney General will eventually provide guidance on how opt-out mechanisms must be designed and implemented.
- Businesses must update their online privacy policy disclosures. Building on existing CalOPPA requirements, the Act requires businesses to explain in their privacy policy the consumers' rights under the Act, the categories of personal information the company has collected from consumers in the last 12 months, and the business purpose for which it has sold or disclosed such information in the last 12 months.

6. The Act will be principally enforced by the California Attorney General. The Act provides for enforcement by the California Attorney General in nearly all instances. Businesses may be liable for civil penalties up to $2,500 per violation after a 30-day cure period, or up to $7,500 for each intentional violation of the Act. This is a notable departure from the earlier draft ballot

initiative, which provided consumers a private right of action.

While there is no private right of action, the Act establishes the right for consumers to bring civil actions where personal information is compromised in a data breach due to a failure to implement reasonable security measures under Cal. Civ. Code 1798.81.5 – subject to a 30-day cure period and provided that the Attorney General declines to prosecute the violation. In the event that a civil action proceeds, the Act provides for statutory damages of $100-$750, or actual damages, whichever is greater.

7. Businesses may incentivize consumers who allow for the sale of their personal information, but may not discriminate against consumers who do not. The Act permits a business to offer financial incentives to consumers for the collection or sale of personal information, and to offer a different price, rate, level or quality of goods and services where "reasonably related" to the value provided to the consumer by use of the consumer's data. Yet, the same section also prohibits a business from discriminating against a consumer for exercising his or her rights (e.g., by charge a different price, or provide a different quality of goods or services). This apparent discrepancy potentially turns on whether the price or service-level discrimination is "reasonably related" to the value provided to the consumer by use of the consumer's data, though it is difficult to understand how this will play out in practice. Indeed, common data-related sales practices (e.g., for interest-based advertising purposes) provide enormous value to the business in terms of revenue generation and market growth compared to the potentially nominal value to consumers of being shown advertisements that are more relevant to their interests. In response to GDPR, we have seen media companies display only a plain text version of their websites to consumers who do not consent to accept cookies. Would this constitute "discrimination" under the California Act?

Some businesses may decide to offer a separate landing page for California consumers. The Act suggests that businesses may choose to maintain a separate homepage dedicated to Californian consumers in order to comply with the requirements of the Act. For example, a business with significant market penetration in the 13-16 year old age bracket may struggle to obtain affirmative authorization from such users before collecting cookie and pixel data on their home pages. A business may face similar challenges in halting the collection of cookie and pixel data for consumers who have opted-out of such data collection or disclosure to third parties. Displaying a homepage stripped of third-party advertising pixels to all Californian consumers may be a more effective method of compliance, though this approach presents its own challenges in whether a business can accurately identify whether an online visitor is coming to the site from California or elsewhere.

Next Steps for Businesses

With the Consumer Privacy Act of 2018, California notched yet another cutting edge win for consumer privacy. A leader on the national privacy scene, California has again set the stage for significant change in the way that companies engage with their customers. While the compliance deadline of January 2020 seems far into the distant future, 1.5 years can pass in the blink of an eye (just ask the thousands of companies who have yet to achieve any level of compliance with the GDPR, which went live on May 25, 2018!). Accordingly, businesses should follow a diligent protocol of assessing their readiness to comply with the Act, identifying gaps between the current compliance posture and desired status, prioritizing remediation activities, and working methodically toward full compliance.

Emily Tabatabai, Antony Kim *and* ***Jennifer Martin*** *are partners in the cybersecurity, privacy and data innovation practice at Orrick, Herrington & Sutcliffe.*