The California Consumer Privacy Act:

Amendments, Regulations and Enforcement

by Daniel Appelman & Alaina Bailey

As of January 1, 2020, all businesses meeting certain criteria that collect, use or sell data of California residents are required to comply with the Act. In a previous client alert, we provided an overview of the sweeping consumer-protective changes that the California legislature enacted to the state's data privacy laws. The reader is encouraged to refer to that overview, as well as to the law itself.

This alert supplements our earlier overview and provides information about:

- the amendments to the CCPA enacted into law subsequent to our earlier client alert;
- the final regulations under the Act that were recently published by the California Attorney General; and
- the enforcement of the CCPA by the California Attorney General.

Covered Businesses

The CCPA's obligations only apply to "covered businesses." A covered business is any for-profit business that collects the personal information of California consumers[1], does business in California, and (i) has annual gross revenue in excess of $25 million, (ii) annually buys, receives, shares or sells the personal information of more than 50,000 California consumers, households or devices for commercial purposes, or (iii) derives 50% or more of its annual revenues from selling consumers' personal information.

The Amendments

Last October, California's Governor Gavin Newsom signed into law six bills that amended the CCPA and California's existing data breach notification statutes. These amendments include the following and help to clarify some of the questions left open in the original version of the Act:

- Enforcement Timing. Consumers may exercise their rights and sue businesses for data breaches[2] as of January 1, 2020. Enforcement by the California Attorney General commenced on July 1, 2020.[3]
- Expanded Scope for Data Breach Notifications. California law requires businesses that possess consumers' personal information to inform those consumers in the event of a breach or other compromise of that information.[4] The new amendments to the data breach notification statutes expand the categories of personal information that, if compromised, would trigger the notification requirement. Those categories now include tax ID numbers, unique ID numbers issued on government documents (*e.g.*, passports, military IDs, etc.) and unique biometric data generated from measurements or technical analysis of human body characteristics (*e.g.*, fingerprints and retina or iris images).
- Data Broker Registration. Data brokers[5] are required to register with the California Attorney General.

The Attorney General's Final Regulations

On June 1, 2020, the California Attorney General submitted his final regulations for the implementation of the CCPA to the California Office of Administrative Law (the "OAL") for approval. He requested expedited review and approval, but the OAL has up to 90 days[6] from the date of submission to do so. Here are some of the notable regulations that we expect to be approved:

Notice Requirements Guidance.

The regulations provide guidance on how covered businesses should provide consumers with notice[7] of their new rights with respect to the collection, use, sale[8] and sharing of their personal information:

Notice in Privacy Policy

Each covered business is required to maintain a general privacy policy that is updated at least every twelve months, is reasonably accessible to consumers (particularly in light of the means and manner of the business's interaction with those consumers) and that discloses the business's practices and policies with respect to the collection, use, sale and sharing of personal information. Under the regulations, this privacy policy must identify or include at a minimum:

- the categories of personal information collected by the business in the preceding 12 months;
- the categories of sources from which such personal information was collected;
- the purpose for collecting or selling such personal information;
- the categories of personal information that the business shared or sold in the preceding 12 months (or a statement that the business made no such sales or disclosures during that period);
- for each category of personal information identified, the categories of third parties with whom the business sells or shares the personal information;
- if the business sells personal information to third parties, notices of such practices and a link to the business's opt-out notice;
- if the business offers a financial incentive or difference in price or service for the collection, retention or sale of personal information, a notice describing the material terms of such program;
- if the business buys, receives, sells or shares the personal information of more than 10 million consumers in a calendar year, a notice (to be disclosed each year by July 1) of the number of consumer requests received, complied with or denied, and the business's average response times for such requests; [9]
- a description of consumers' individual rights with respect to their personal information;
- how consumers, or their authorized agents, may submit requests to exercise their rights (and the information required to do so);
- a general description of the business's process for verifying consumer requests;
- a statement on whether the business has actual knowledge that it sells personal information of minors under 16 years of age;
- who to contact with questions or concerns about the business's privacy practices; and
- the date the policy was last revised.

Notice at Collection of Personal Information

Each covered business is required to provide consumers with separate written notice prior to or at the time of collecting personal information. This notice must identify the categories of information collected, the purposes for its use by category and must contain links to the business's general privacy policy and opt-out notice. This notice must be readily accessible where consumers will encounter it and must be given whenever and wherever the business collects personal information, including in offline situations.

When a business collects personal information from a consumer's mobile device for purposes that the consumer would not reasonably expect, the business must also provide a pop-up at the point of collection that

summarizes the personal information collected and provides a link to the full collection notice.[10]

Notice of Right to Opt-Out

If a covered business sells personal information, it must provide a link titled "Do Not Sell My Personal Information" or "Do Not Sell My Info," which directs consumers to a publicly available webpage that gives notice that they have the right to opt-out of any sale of their personal information. This notice must include an interactive form or instructions by which consumers can submit their requests to opt-out. The regulations require that the links to this notice appear on the business's homepage(s)[11]. If a business substantially interacts with consumers offline, it must also provide notice by an offline method (*e.g.*, with paper versions of the notice or prominent signage directing consumers to where the notice can be found online).

Notice of Financial Incentive

If a covered business offers a program with a financial incentive or price or service differences to get consumers to submit to the collection, retention or sale of their personal information, that business must provide a written notice of such practices where consumers will encounter the notice before opting into the program. The notice must provide a succinct summary of the program as well as a description of the material terms of such financial incentive, price or service differences. The notice must also provide consumers with a method to opt-in and out of the program, with a statement of the consumers' right to withdraw at any time.

General Requirements for All Notices

Regardless of the type of notice required by the Act, all notices must:

- use plain, straightforward language and avoid technical or legal jargon;
- use a format that draws the consumers' attention to the notice and makes the notice readable, including on smaller screens (if applicable);
- be available in all languages in which a business operates or provides other information to its consumers; and
- be accessible to consumers with disabilities. For notices provided online, a business must follow generally recognized industry standards, such as version 2.1 of the accessibility guidelines offered by the World Wide Web Consortium.

Verifying and Responding to Consumer Requests to Exercise their CCPA Rights.

Under the CCPA, consumers must submit formal requests[12] to a covered business in order to exercise certain rights with respect to personal information, such as the right to access that information and the right to have that information deleted.

Specifically, each business is required to: (i) implement mechanisms to enable it to receive such requests; (ii) timely confirm the receipt of such requests; (iii) properly verify the identity of the requesting consumers; and (iv) respond in a timely fashion to such requests by either fulfilling the requests or informing the requesting consumers of the reasons for not doing so.

The regulations set forth the required procedures for verifying the legitimacy of, and responding to, such consumer requests. Each business must establish, document and comply with reasonable verification methods and closely tailor such methods to its specific practices by considering:

- the type, sensitivity and value of the personal information collected and maintained about consumers;
- the risk of harm to consumers posed by any unauthorized access or deletion;
- the likelihood that fraudulent or malicious actors would seek the personal information;
- whether the personal information needed to facilitate verification is sufficiently robust to protect against fraudulent requests;
- the manner in which the business interacts with consumers; and
- the technology available for verification.

In addition, the regulations establish the following:

- minimum requirements for the methods a business must offer consumers to enable them to submit requests to exercise their rights under the CCPA;[13]
- a business must confirm receipt of requests and provide information about how the business will process and respond to the request within 10 days;
- a business must act on verified requests within 45 days from the date of receipt (not from the date of verification), unless extended as permitted by the regulations;
- a business must implement reasonable security measures to detect fraudulent identity-verification activity and prevent the unauthorized access to or deletion of consumers' personal information;
- a business must establish training procedures for all individuals responsible for handling consumer inquiries regarding the business's privacy practices and CCPA compliance; and
- a business must maintain records of all consumer requests, and the business's responses to such requests, for at least 24 months from the date of receipt.

Recommendations

The Attorney General signaled an intent to defer to businesses that make good faith efforts to comply with their CCPA obligations, while also making examples of businesses that do not.[14] Each covered business should promptly implement procedures to comply with the Act's requirements. At a minimum, these should include:

- updating your business's privacy policy to inform consumers of their new rights (and revisiting it annually);
- if applicable, providing links to the notice that describes consumers' right to opt-out of the sale of their information on your business's website and in your business's privacy policy titled "Do Not Sell My Personal Information" or "Do Not Sell My Info;"
- implementing procedures to receive, verify and respond to consumers' CCPA requests in accordance with the Act's minimum requirements;
- implementing procedures to track consumers' CCPA requests and train individuals responsible for handling those requests; and
- reviewing and assessing whether your business's current data security policies and practices are sufficient to meet the Act's requirement to implement reasonable security measures.

[1] A "consumer" is defined as any natural personal who is a California resident. Cal. Civ. Code § 1798.140(g).

[2] The CCPA provides a private right of action for the unauthorized access, theft or disclosure of nonencrypted and nonredacted personal information due to a business's failure to implement reasonable security practices and procedures that are appropriate for the particular type of personal information involved. Cal. Civ. Code § 1798.150.

[3] The California Attorney General confirmed that enforcement of the CCPA began as of July 1, 2020, despite the absence of approval for the final regulations. *See* Attorney General Becerra Issues Statement on Day One of CCPA Enforcement: Know Your Responsibilities, July 1, 2020, https://oag.ca.gov/news/press-releases/attorney-general-becerra-issues-statement-day-one-ccpa-enforcement-know-your.

[4] Cal. Civ. Code § 1798.82(a).

[5] A "data broker" is defined as a business that knowingly collects and sells to third parties the personal information of a consumer with whom the business does not have a direct relationship. Cal. Civ. Code § 1798.99.80(d).

[6] On March 30, 2020, Governor Gavin Newsom signed Executive Order N-40-20 in response to the COVID-19 pandemic. This executive order, among other things, extended the OAL's deadline to review the CCPA regulations for an additional 60 days beyond the original 30-day deadline.

[7] *See* 11 C.C.R. §§ 999.304-999.308 (final draft).

[8] The concept of a "sale" under the CCPA is broadly defined to include any communication of a consumer's personal information for monetary or other valuable consideration; which encompasses activity that businesses may not consider as traditional sales (*e.g.*, using cookies to enable targeted advertising to specific customers). *See* Cal. Civ. Code § 1798.140(t).

[9] *See* 11 C.C.R. § 999.317(g) (final draft).

[10] *See* 11 C.C.R. § 999.305(a)(4) (final draft) for examples of scenarios in which this pop-up or "just-in-time" notice is required.

[11] An internet homepage can include a website's splash or landing page, any webpage that collects personal information, and, in the case of an online service, the platform's download page or a link within the application's configuration (*e.g.*, an "About" or "Information" page). Cal. Civ. Code § 1798.140(l).

[12] Businesses are only required to respond to "verifiable consumer requests." A "verifiable consumer request" is defined as a request that a consumer (or someone legitimately acting on the consumer's behalf) makes that a business can reasonably verify is from the consumer about whom it collected personal information. Cal. Civ. Code § 1798.140(y).

[13] *See* 11 C.C.R. § 999.312 (final draft).

[14] *See* Nandita Bose, *California AG says privacy law enforcement to be guided by willingness to comply*, Reuters Technology News (December 10, 2019), https://www.reuters.com/article/us-usa-privacy-california/california-ag-says-privacy-law-enforcement-to-be-guided-by-willingness-to-comply-idUSKBN1YE2C4.