Published on *The National Law Review* https://natlawreview.com

On the Verge of CCPA Enforcement: What Should Companies Do to Comply?

Article By:

Alaap B. Shah

On January 1, 2020 California Consumer Privacy Act ("CCPA") largely came into effect, albeit with several last-minute modifications and a need to promulgate regulations. As our colleagues have discussed previously here, CCPA joins other California laws safeguarding California residents' privacy rights under the California Constitution. Despite uncertainty around the final regulatory parameters of the law, CCPA grants the California Attorney General (AG) the authority to begin enforcement on July 1, 2020. Further, there have been no indications that such enforcement will be delayed.

Re-issued Proposed CCPA Regulations

After the California legislature passed several amendments to the CCPA in October 2019, the California AG has been working on proposed regulations. The proposed regulations, initially introduced on October 12, 2019, went through three rounds of comment periods and were recently amended and reissued as the "Final Text of Regulations" on June 1, 2020. These proposed regulations notably add new aspects and regulatory hurdles to CCPA implementation most notably: (i) increasing requirements for initial notices; and (ii) adding new requirements on the contents in business's privacy policies. These reissued proposed regulations were submitted to the California Office of Administrative Law (OAL) for review. The OAL has thirty working days to review these regulations, plus an additional sixty calendar days under the California Governor's Executive Order N-40-20related to the COVID-19 pandemic, to review the regulations for procedural compliance with state law.

CCPA Proposed Regulatory Framework

The CCPA applies to any for-profit business that: (i) collects personal information on California residents; (ii) does business in the state of California; and (iii) satisfies one or more of the following thresholds: (a) has annual gross revenues in excess of $25,000,000; (b) alone or in combination, annually buys, receives for the business's commercial purposes, sells, or shares for commercial purposes, alone or in combination, the personal information of 50,000 or more consumers, households, or devices; or (c) derives 50 percent or more of its annual revenues from selling consumers' personal information. Businesses that hit the thresholds will be covered even if they are located outside the state of California.

Notably, companies subject to CCPA must “at or before the point of collection” of personal information provide notice to consumers informing them of the categories of personal information the company collects and what purpose the information is used by the company. In addition, CCPA requires businesses to post a clear and conspicuous link on their website that says “Do Not Sell My Personal Information” and then to enable consumers to opt-out of the sale of their data to third parties. CCPA also establishes a wide-range of rights to consumers (as specified below). Companies should be aware of the potential added cost of business in responding to these rights and ensure that they do not discriminate against any individual who exercises their rights under CCPA.

CCPA also establishes robust consumer rights for Californians including:

- to know what personal information is being collected about them;
- to know whether their personal information is sold or disclosed and to whom;
- to opt-out of the sale of their personal information;
- to access their personal information and receive a copy;
- to be free from discrimination for exercising their privacy rights;
- to the deletion of their personal information, subject to certain exceptions; and
- to bring a private right of action if certain personal information is subject to unauthorized access and exfiltration, theft, or disclosure as a result of the business’s violation of the duty to implement and maintain reasonable cybersecurity procedures and practices.

Companies that fail to follow CCPA could face significant monetary penalties. First, noncompliance could result in civil penalties ranging from $2,500 for non-intentional violations up to $7,500 for intentional violations. Second, violators could face liability under private rights of action ranging between $100 to $750 per consumer, per violation. If actual damages to consumers are in excess of $750 per consumer, per violation, the AG also has the discretion to increase the amount of damages. In class action scenarios, penalties have the potential to exponentially increase costs to businesses, especially when compared to previous breaches or privacy violations.

CCPA Impact on Healthcare and Life Sciences Companies

Despite the CCPA’s broad scope and reach, the law does include several notable exemptions that are germane to healthcare and life sciences companies. Particularly, CCPA does not govern the collection, use, disclosure or protection of (1) medical information governed by the California Confidentiality of Medical Information Act (CMIA), (ii) protected health information governed by the Health Insurance Portability and Accountability Act (HIPAA) and the Health Information Technology for Economic and Clinical Health Act (HITECH); or (iii) information collected as part of a clinical trial subject to the Federal Policy for the Protection of Human Subjects (also known as the Common rule)

pursuant to good clinical practice guidelines issued by the International Council for Harmonisation or pursuant to human subject protection requirements of the U.S. Food and Drug Administration.

Nevertheless, it is important to keep in mind that these exemptions do not cover all personal information collected by healthcare and life sciences businesses. For example, marketing or employment data collected by businesses that operate in these areas may be subject to CCPA. Additionally, operational considerations regarding how a company collects and maintains its data may warrant voluntary application of the CCPA requirements for efficiency and consistency reasons.

How to Prepare for CCPA Enforcement

As a result of CCPA and other data protection laws, privacy and data security compliance programs should be agile to address these new or expanded demands quickly. With CCPA's July 1, 2020 enforcement deadline, steps that can be immediately taken may include, but are not limited to, the following:

- updating notices and privacy policies;
- reviewing data flows including data mapping and classification;
- segregating data and IT systems between regulated and non-regulated data repositories;
- implementing cookie banners and web beacons in accordance with CCPA-compliant privacy policies;
- implementing individual request processes (including opt-out and deletion); and
- implementing training to meet CCPA's new requirements.

CCPA Compliance in the Age of COVID-19

As a result of the COVID-19 pandemic, many businesses may collect, store and process additional information about Californians in order to help mitigate the spread of the disease. As such, CCPA may impose additional regulatory burdens on businesses relative to such information. If your business is collecting additional COVID-19 related personal information beyond what it typically would, there are several considerations to keep in mind. First, consider where any such information is stored. Second, evaluate how that information is being protected. Third, identify if that information is being shared, and with whom. Fourth, determine all the legitimate purposes (primary and secondary) for collection of the information. Subsequently, businesses should update privacy policies and notices, and provide such documents to employees and consumers prior to beginning any new or expanded collection of personal information.

To help navigate CCPA's impending enforcement data of July 1, 2020, especially in the context of the current health crisis, it is recommended you consult legal counsel.

National Law Review, Volume X, Number 174

Source URL:https://natlawreview.com/article/verge-ccpa-enforcement-what-should-companies-do-to-comply