CCPA Private Litigation, Recent Developments and Potential New Privacy Legislation on the Horizon

By Jim Snell, Marina Gatto and Gabriella Gallego[1]

The California Consumer Privacy Act (CCPA) went into effect over five months ago, on January 1, 2020. Although enforcement by the California Attorney General cannot begin until July 1, private plaintiffs have been bringing claims under the law's limited private right of action since before the beginning of the year.

In addition, the California Attorney General has been working on regulations that are now in final form but still not effective and may not be effective until after the July 1 date by which Attorney General enforcement can begin. Companies are struggling to work on compliance with just finalized but still not legally enforceable regulations.

Further, there have been efforts to put a ballot initiative on the November ballot that would substantially amend the CCPA.

This article will (1) discuss CCPA private litigation trends to date, (2) summarize the California Attorney General regulations and (3) summarize a ballot initiative that may be on the November 2020 ballot.

CCPA Litigation and the Private Right of Action

The CCPA provides a limited private right of action for data breaches affecting certain categories of personal information where the breach is the result of a lack of reasonable security. More specifically, section 1798.150(a)(1)(A) of the CCPA states that a private litigant may bring a cause of action only if their "nonencrypted and nonredacted personal information . . . is subject to an unauthorized access and exfiltration, theft, or disclosure as a result of the business's 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." Several of the private complaints filed thus far allege claims under this section of the CCPA; however, private claims also allege violations of the CCPA not subject to the private right of action as well as claims for violations of other laws by referencing alleged CCPA violations. For example, in response to an alleged data breach by online video communications company Zoom, a plaintiff alleges a CCPA claim under the private right of action--that Zoom failed to implement reasonable security standards which resulted in the unauthorized disclosure of unredacted personal information. Complaint at 11, *Robert Cullen v. Zoom Video Commc'ns, Inc.*, No. 5:20-cv-02155 SVK (N.D. Cal. filed March 3, 2020). However, the plaintiff also alleges violations outside of the private right of action, including that Zoom allegedly violated the CCPA "by, among other things, collecting and using personal information without providing consumers with

[1] Partner James Snell represents clients in a wide range of complex commercial matters, including privacy and security, internet, marketing, and intellectual property litigation. Associates Marina Gatto and Gabriella Gallego assist companies with data security and privacy compliance matters, including compliance with the California Consumer Privacy Act (CCPA) and the General Data Protection Regulation (GDPR). Jim, Marina and Gabriella are all based in Perkins Coie's Palo Alto office.

adequate notice consistent with the CCPA, in violation of Civil Code section 1798.100(b)." *Id.* at 10. While § 1798.100(b) is a requirement of the CCPA, it is expressly not one that a private litigant is permitted to enforce. *See* Civil Code 1798.150 ("The cause of action established by this section shall apply only to violations as defined in subdivision (a) and shall not be based on violations of any other section of this title.").

Similarly, in *Johnston v. Zoom Video Communications, Inc.*, No. 5:20-cv-02376 (N.D. Cal. filed Apr. 8, 2020), Johnston alleges that Zoom violated the CCPA by using personal information of the alleged class without providing the notice required by § 1798.100(b) (categories and purposes of PI collection) and § 1798.120(b) (right to opt-out of sale) and for false and deceptive behavior regarding Zoom's sale of data. Johnston claims that Zoom's affirmative statements in its privacy policy that it **does not** sell user data are inaccurate. Again, these claims are not permitted to be brought by a private plaintiff under the CCPA, but were nevertheless made.

In addition to limiting private CCPA claims to a narrow category of data breach cases, the CCPA also explicitly limits a claimant's rights to assert CCPA violations under other claims. Specifically, the CCPA provides that "nothing in this title shall be interpreted to serve as the basis for a private right of action under any other law." 1798.150(C). Despite this restriction, plaintiffs have filed cases alleging CCPA violations as the basis for other claims, including, for example, violations of the California Unfair Competition Law (UCL) (codified at Cal. Bus & Prof. Code §§ 17200 et seq.). *See, e.g.*, Complaint, *Cullen*, No. 5:20-cv-02155 SVK; Complaint, *Burke v. Clearview AI, Inc.*, No. 3:20-cv-00370 BAS MSB (S.D. Cal. filed Feb. 27, 2020); Complaint, *Almeida v. Slickwraps Inc.*, No. 2:20-cv-00559-TNL-CKD (E.D. Cal. filed Mar. 12, 2020); Complaint, *Dennis v. First Am. Title Co.*, No. 8:19-cv-01305 (C.D. Cal. filed July 1, 2019) (class action suit alluding to defendant's reference to the CCPA in its 10-K filings in support of plaintiff's UCL claim). CCPA violations have also been asserted under intrusion upon seclusion and constitutional privacy grounds.

The lesson from these cases is that plaintiffs are asserting the CCPA broadly and that it will be the job of the courts to apply the law in the narrow way the private right of action was intended. Given how recently such cases have been filed, and given the court delays resulting from the Covid-19 pandemic, we have yet to see orders from courts narrowing these cases. While we await such orders, companies should expect and plan for broad allegations to be brought forth, and consider steps to minimize such claims from private plaintiffs.

Modifications to the Draft Regulations

In addition to the evolving private CCPA litigation, the California Attorney General has been preparing for CCPA enforcement which will begin on July 1, 2020, and has also recently finalized the CCPA regulations. The Attorney General has also made clear in a press release that he will not postpone enforcement of the statute despite the global COVID-19 pandemic, reminding California residents that it is "more important than ever for Californians to know their privacy rights." As such, companies should expect Attorney General enforcement to begin July 1, 2020.

The Attorney General has also been working on CCPA regulations for more than a year, and submitted final regulations to the Office of Administrative Law (OAL) on June 1, 2020. The

OAL has 30 working days plus an additional 60 calendar days to determine whether the regulations satisfy the procedural requirements of the Administrative Procedure Act, though the Attorney General has asked that review be expedited so the regulations can be final by the July 1, 2020 enforcement date. Once approved, the final regulations will be filed with the Secretary of State and become enforceable. One question is how the Attorney General will view enforcement of the CCPA before the regulations are effective, and we speculate that initial enforcement may focus on the language of the CCPA itself, with enforcement of the regulations to follow, after they become effective. In the meantime, companies are working to incorporate the recently finalized regulations into their compliance programs.

The final regulations contain additional important detail, including a provision that states that a violation of the regulations shall be deemed a violation of the CCPA. While a careful review should be made of the regulations, we highlight four areas below that companies should consider.

Privacy Policy Requirements

The final regulations contain additional guidance and requirements for what should be included in a business's privacy policy. Among other things, the regulations require that "[f]or each category of personal information" disclosed or sold, the business also list "the categories of third parties to whom the information was disclosed or sold." Cal. Code Regs. tit. 11, § 999.308(c)(1)(g)(2). The regulations also require that a privacy policy contain the date it was last updated as well as information whereby a consumer with a question or concern about the business's privacy policy and practices can contact the business "using a method reflecting the manner in which the business primarily interacts with the consumer." Id. § 999.308(c)(6)-(7).

A privacy policy must also include instructions on how an authorized agent can make a request on behalf of a consumer, as well as details regarding how the business will verify the consumer's request.

Methods for *Verification*

One of the biggest challenges businesses are facing with the sudden influx of consumer rights requests is how to verify requests. The final regulations provide some guidance as to how businesses should approach verifying consumer requests. For example, the regulations would give businesses the explicit ability to deny requests that cannot be verified within 45 days. Id. § 999.313(b). The regulations also state that a business "shall not" respond to access requests for specific pieces of information that cannot be verified. *Id.* §999.325(f). Two examples are provided for how a business could comply with this requirement. One example specifies that a retailer that maintains purchase history information may require the consumer to identify his or her recent purchases, or the dollar amount of his or her most recent purchase. *Id.* §999.325(e)(1). However, if a business is not engaged in retail but maintains a mobile app, a suggested verification method is to ask consumers to provide information that only the person using the mobile app would know, or require they respond to a notification sent to their device. Id. § 999.325(e)(2). The Attorney General also addressed verification requirements for consumers submitting rights requests through authorized agents by stating that businesses may "directly confirm" with the consumer that he or she did in fact grant the agent signed permission to submit

a request on his or her behalf. This addition may help businesses avoid phony authorized agent requests that have not in fact been authorized by a consumer.

Service Providers Rights and Restrictions

The Regulations also clarify some of the rights and restrictions related to service providers. Specifically, the regulations identify five ways service providers may use, retain, or disclose personal information, including: (1) "[t]o process or maintain personal information on behalf of the business that provided the personal information, or that directed the service provider to collect the personal information, and in compliance with the written contract for services required by the CCPA"; (2) "[t]o retain or employ another service provider as a subcontractor"; (3) "[f]or internal use by the service provider to build or improve the quality of its services," provided, however, that the "use does not include building or modifying household or consumer profiles to use in providing services to another business, or correcting or augmenting data acquired from another source." *Id.* § 999.314(c)(1)-(3).

Notice Requirements

The Regulations impose additional notice requirements that should be reviewed carefully. The regulations also attempt to clarify some ambiguity in the CCPA as to who needs to provide notice. For example, the Regulations confirm that data brokers who may not have a means of providing notice "at or before the point of collection," are not required to provide such notice so long as they include in their registration with the Attorney General a link to their online privacy policy that includes instructions on how a consumer can submit an opt-out request. *Id.* § 999.305(e).

Financial Incentives

The Regulations include detailed requirements regarding financial incentives and price or service differences related to the collection, retention, or sale of personal information. These provisions require disclosures that include opt-in and opt-out rights, specific notice requirements, as well as anti-discrimination provisions. These provisions should be carefully reviewed by any business who may be providing financial incentives, and we recommend that such review take place under privilege given the ambiguity that exists in the CCPA and the Regulations regarding financial incentives.

Potential New Legislation: The California Privacy Rights Act

There is also another piece of legislation potentially on the horizon in 2021. The California Privacy Rights Act ("CPRA") is a ballot initiative that is authored by the same individual whose efforts in 2018 resulted in the California legislature enacting the CCPA. At the time of writing this article the future of the CPRA remains unclear, although it may be likely that this initiative will appear on the November 2020 ballot. Although the signatures gathered to place this initiative on the ballot have yet to be verified by the Secretary of State, one thing that is for certain is that if enacted, the CPRA would amend the CCPA in several significant ways, some of which we discuss below.

Creation of a New State Agency

The CPRA would create the California Privacy Protection Agency (the "Agency") which could potentially dramatically impact regulatory enforcement of the CCPA in California. The Agency would be responsible for enforcing the CPRA through administrative enforcement actions. Decisions resulting from such actions would be subject to judicial review in an action brought by an interested party and subject to an abuse of discretion standard.

Rulemaking power would also be transferred from the California Attorney General to the Agency on the later of July 1, 2021, or 6 months after the Agency provided notice to the Attorney General that it was prepared to begin rulemaking.

New Right to Correction

The CPRA would also give consumers new rights, such as the right to request that a business that maintains their personal information correct such inaccurate personal information. Businesses would also be required to disclose to consumers the right to make such a request, and upon receiving a request use commercially reasonable efforts to correct the inaccurate personal information at issue.

New Requirements for Sensitive Personal Information

The CPRA would also create the newly defined term "sensitive personal information," which would include personal information that reveals a consumer's social security number, driver's license or state identification card number, account login information, financial account information, precise geolocation, racial or ethnic origin or religious beliefs, in addition to other information. Consumers would also be given new rights with respect to their sensitive personal information, including the right to limit the use and disclosure of their sensitive personal information and the right to be informed at or before the point of collection as to the categories of sensitive personal information to be collected and the purposes for which the categories will be used and whether such information is sold or shared, in addition to the length of time the business intends to retain each category of sensitive personal information.

Broader Time Frame for Access Rights

The CPRA would also go beyond what is currently required under the CCPA by extending the look-back period for a consumer's right to request access to their personal information. With respect to personal information collected on or after January 1, 2022, the CPRA provides that a consumer can request that "the business disclose the required information beyond the 12-month period and the business shall be required to provide such information unless doing so proves impossible or would involve a disproportionate effort."

Added Clarity

In addition to imposing new obligations on businesses, the CPRA would also provide some additional clarity. For example, the CPRA would make clear that a business's requirement to disclose certain information upon request will not require a business to disclose trade secret information. The CPRA would also make clear that the right to be free from discrimination is not

absolute, and that a business is not prohibited from "offering loyalty, rewards, premium features, discounts, or club card programs consistent with this title."

Purpose Limitations

The CPRA would also limit a business's collection, use, retention, and sharing of a consumer's personal information to that which is "reasonably necessary and proportionate to achieve the purposes for which the personal information was collected or processed, or for another disclosed purpose that is compatible with the context in which the personal information was collected, and not further processed in a manner that is incompatible with those purposes." Therefore, a business would not be allowed to retain a consumer's personal information or sensitive personal information for longer than is reasonably necessary for the purpose for which the business disclosed that the personal information was being collected.

Additional Opt-Out Mechanisms

The CPRA would broaden the opt-out rights that California consumers are currently afforded by extending such opt-out rights beyond personal information "sold," to include the right to opt-out of the "sharing" of personal information and the right to opt-out of the disclosure and use of "sensitive personal information." "Sharing" is defined under the CPRA to include "sharing, renting, releasing, disclosing, disseminating, making available, transferring, or otherwise communicating orally, in writing, or by electronic or other means, a consumer's personal information by the business to a third party for cross-context behavioral advertising, whether or not for monetary or other valuable consideration, including transactions between a business and a third party for cross-context behavioral advertising for the benefit of a business in which no money is exchanged."