Articles + Publications | November 16, 2020

The Murky Waters of the CCPA's Private Right of Action: Real and Perceived Ambiguities Complicating Litigation

Privacy & Cybersecurity Newsletter

WRITTEN BY

Tara L. Trifon | Lindsey E. Kress

The California Consumer Privacy Act ("CCPA") gives individuals the right to seek statutory damages against a business in limited circumstances involving the CCPA's reasonable security obligation. *See* Cal. Civ. Code § 1798.150. There have been dozens of lawsuits filed since the CCPA became effective, with the first complaint filed on February 3, 2020. Courts have not yet decided any dispositive motions in these lawsuits, so it is unclear whether, and to what extent, these claims will be deemed sustainable. Part of the difficulty for businesses attempting to navigate the CCPA is that, absent further legislative amendments, the private right of action provision in the CCPA contains numerous ambiguities that will need to be clarified by the courts.

Who can exercise the private right of action?

The CCPA defines the term "consumer" as a "natural person who is a California resident . . . however identified, including by any unique identifier." Cal. Civ. Code § 1798.140(g). A California resident includes people who are in California for "other than a temporary or transitory purpose." Cal. Code Regs., tit. 18, § 17014, subd. (a). The definition also includes people who are domiciled in California but live outside the state for a "temporary or transitory purpose." *Id*.

The "temporary or transitory purpose" analysis requires a factual determination of the location "with which a person has the closest connection during the taxable year." Cal. Code Regs., tit. 18, § 17014, subd. (b). Considerations will include whether the person is in California for less than six months and/or for a finite period of time, and whether the person maintains a permanent abode in a different state. *Id*.

For the most part, it may be relatively simple to establish that someone is, or is not, a "consumer" for purposes of the CCPA. For instance, the first case to raise this residency issue is *Fuentes v. Sunshine Behavioral Health Group LLC*, Civil Docket No. 8:20-cv-00487-JLS-JDE (C.D. Cal. 2020), where the plaintiff admits he is a Pennsylvania resident and was only in California at the defendant's facility for one month to improve his health, which is almost certainly insufficient to meet the CCPA's residency requirement. However, there may be large groups of people, like boarding school or college students, for whom the "temporary or transitory purpose" analysis is more complicated and whose residency is therefore more difficult to determine.

When can a consumer assert a claim under the CCPA?

California residents have the right to bring a lawsuit under the CCPA only in certain circumstances. Specifically, the consumer must demonstrate that "nonencrypted and nonredacted personal information . . . [was] 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." Cal. Civ. Code § 1798.150(a)(1). The statute prohibits individuals from asserting any other types of violations under the CCPA. *See* Cal. Civ. Code § 1798.150(c).

As a threshold matter, there is no consensus over whether the CCPA only allows a consumer to file a lawsuit after a data breach or whether the statute can be construed more broadly. The guidance from the California Attorney General suggests that the former is the correct interpretation: "[a consumer] can only sue a business under the CCPA if there is a data breach, and even then, only under limited circumstances."[1] Conversely, plaintiffs are taking a more expansive view of what constitutes "unauthorized access and exfiltration, theft, or disclosure," alleging that a business violates the CCPA when it shares a consumer's personal information with a third party without the consumer's consent. *See e.g., Cullen v. Zoom Video Communications, Inc*., Civil Docket No. 5:20-cv-02155-LHK (N.D. Cal.) (wherein the plaintiffs initially alleged that Zoom violated the CCPA by improperly sharing their personal information with Facebook, Inc., though this claim was ultimately dropped from the recently amended complaint); *G.R. v. TikTok Inc., et al*., Civil Docket No. 1:20-cv-05212 (N.D. Ill.) (alleging that TikTok disclosed and/or disseminated biometic identifiers or biometric information to third parties without the plaintiff's consent). The CCPA claims against Zoom and TikTok have now been resolved (either by withdrawal of the claim or by a proposed settlement), but plaintiffs will undoubtedly continue trying to test the limits of the private cause of action.

The consumer's information that was accessed and disclosed must also be nonencrypted, nonredacted, and personal. In particular, the information at issue must include the consumer's first name (or first initial) and last name in combination with at least one of the following: (1) social security number, (2) driver's license number or California identification card number, (3) account number or credit/debit card number along with any security code, access code, or password, (4) medical information, (5) health insurance information, or (6) unique biometric data (such as fingerprints). *See* Cal. Civ. Code § 1798.150(a)(1) (citing "personal information" defined under Cal. Civ. Code § 1798.81.5(d)(1)(A)). Nonetheless, plaintiffs are attempting to enlarge the type of information that could give rise to a CCPA claim. *See e.g., Rahman v. Marriot International, Inc.*, Civil Docket No. 8:20-cv-00654-DOC-KES (C.D. Cal.) (relying on the more extensive definition of personal information set forth in Cal. Civ. Code § 1798.140(o)(1) to support the CCPA claim). In view of such attempts, it remains to be seen whether courts will apply the definition of personal information narrowly and in conformance with the statute.

Lastly, the disclosure of the personal information must have been due to the business's violation of its duty to implement and maintain "reasonable security procedures and practices." Without question, this provision is the vaguest requirement that an individual claimant must establish in order to pursue a CCPA cause of action. The statute is silent as to what practices or procedures a business may employ to meet satisfy this requirement. Additionally, the California Attorney General declined to provide any guidance in the regulations, despite being requested to do so.[2] Without further clarification from the legislature or the California Attorney General, this provision of the CCPA's private cause of action is likely to lead to significant amounts of litigation.

Conclusion

Litigation under the CCPA is just getting started. In the months since the first complaint was filed, plaintiffs have plainly attempted to expand the scope of the private cause of action provision beyond what may have been the legislature's original intent. Cases to date have not provided any notable insights as all of the lawsuits are still in their beginning stages and/or the parties are actively engaged in settlement negotiations. In addition, the CCPA regulations that became effective on August 14, 2020, fail to provide any guidance for businesses attempting to navigate the implementation of the CCPA. Thus, businesses will likely continue to face questionable claims asserted by plaintiffs until a court decision can provide some direction. Because parties tend to engage in early settlement negotiations when dealing with class actions, we may be in for a long wait.

---

[1] *See* https://oag.ca.gov/privacy/ccpa (last accessed 10/3/2020).

[2] *See* https://oag.ca.gov/sites/all/files/agweb/pdfs/privacy/ccpa-fsor-appendix-a.pdf (last accessed 10/4/2020), Response # 924 (stating that it would be too limiting to prescribe reasonable security measures and that "whether a business uses reasonable security measures when transmitting personal information to the consumer is a fact-specific determination.").

RELATED INDUSTRIES + PRACTICES

- Privacy + Cyber