Data Privacy in California: Enforcement and Litigation Under The California Consumer Privacy Act

Business Law Journal
By Lana Milojevic, CIPP/US and Brian Wheeler on 02.11.2020

The California Consumer Privacy Act (CCPA) went into effect on January 1, 2020. Is your business prepared and in compliance with the new law?

In Parts One through Three of our CCPA series, we provided an overview of the law:


Part 2: Consumer Rights Under The California Consumer Privacy Act

Part 3: Practical Steps You Can Take Now Before the CCPA Goes Into Effect

In this Part Four of our series, we review the Attorney General’s enforcement mechanisms under the CCPA and the Attorney General’s proposed regulations, as well as potential litigation by consumers pursuant to the private rights of action under the CCPA and other California consumer protection laws.

The potential issues, costs, and risks in regulatory enforcement and litigation can be expansive, and we cannot cover in full detail here all of the rights, obligations, and requirements that may impact your organization, so always consult counsel with any specific questions relating to your particular business and its associated risks.

Enforcement by the Attorney General under the CCPA and the Attorney General’s Regulations

The CCPA is designed to vest primary enforcement responsibility of its terms and any violations on the California Attorney General. The CCPA imposes civil penalties ranging from $2,500 to as much as $7,500 per violation, if the violation was intentional.
Data Privacy in California: Enforcement and Litigation Under The California Consumer Privacy Act

In October 2019, the Attorney General’s office released draft proposed regulations to attempt to answer some of the many questions surrounding the CCPA and clarify businesses’ obligations. However, critics of the regulations have argued that the proposed regulations only add to the confusion surrounding CCPA compliance and enforcement, not help it. The final regulations are expected by July 1, 2020.

Formal enforcement proceeding by the California Attorney General will also not begin until July 1, 2020. What remains unclear, however, is whether the agency will retroactively pursue violations that occur between January 1 and July 1, 2020, even though the Attorney General’s regulations will not be final until July 1, 2020. Indeed, the Attorney General’s office has not foreclosed the possibility that it may seek penalties for violations that occur after the CCPA’s effective date during this time that its regulations are only in their draft form.

Attorney General Xavier Becerra has previously indicated that the Office “will look kindly on those that … demonstrate an effort to comply,” with the requirements of the CCPA, so even if your business has not completed, or even started, CCPA compliance efforts, it is not too late to mitigate your CCPA risk.

Private Actions by Consumers

As is often the case with California consumer protection laws, a further—and sometimes even greater—threat to non-compliant companies will likely come from the very active California plaintiffs’ bar and consumers themselves in the form of individual and putative class action litigation.

Among its other enforcement provisions, the CCPA grants a private right of action to consumers for data breaches. But unlike existing causes of action for data breaches, the CCPA private right of action authorizes statutory damages and is not limited to actual damages only. The CCPA allows consumers to recover the greater of their actual damages or statutory damages ranging from $100 to $750 per consumer per incident. This sets the stage for a potential new wave of private attorney general representative actions akin to the proliferation of representative wage and hour claims that California employers have seen under the Private Attorneys General Act of 2004 (“PAGA”). Moreover, because the courts have not yet had the opportunity to set the boundaries of the CCPA’s private right of action and potential enforcement under other catch-all private rights of action and attorneys’ general statutes, we expect the legal landscape and case law governing enforcement actions to develop rapidly and further shape the scope of the private right of action under the CCPA.

Plaintiffs could also attempt to utilize the California Unfair Competition Law (“UCL”) to enforce the CCPA by bootstrapping violations of the CCPA into a UCL claim. The UCL generally allows plaintiffs to enforce other statutory rights where they can show they have suffered harm or losses as a result of unlawful, unfair, or fraudulent practices. In this manner, the UCL broadly allows plaintiffs to “borrow” violations of other statutes and treats those alleged violations as independently actionable unfair or unlawful practices. While plaintiffs are generally prohibited from using the UCL to plead around an absolute bar to private relief, we have seen litigants test and push the boundaries of these limits in recent years and can expect that trend to continue.
Data Privacy in California: Enforcement and Litigation Under The California Consumer Privacy Act

Plaintiffs in at least one recently filed federal class action have already relied on the CCPA to support their UCL claim. In *Barnes v. Hanna Andersson, LLC*, No. 20-cv-00812, filed on February 3, 2020, in the United States District Court for the Northern District of California in San Francisco, the plaintiff sued Salesforce.com Inc. and Hanna Andersson LLC, a children’s clothing company, for violation of the UCL based in part on the defendants’ alleged failure to comply with the requirements of the CCPA. Plaintiffs allege that the defendants failed to protect user data, safeguard their platforms or provide cybersecurity warnings, and that these actions constituted unfair practices because they violated California state laws, including the CCPA.

The lead plaintiff in *Barnes* is a California resident who alleges she was a victim of a data breach after Hanna Andersson was hacked, resulting in the compromise of her and other consumers’ personal information, including names, payment details, and addresses. The breach was allegedly not discovered until law enforcement found the hacked customer information for sale on the dark web. The complaint further alleges that the information was hosted by Salesforce on its e-commerce platform, which was allegedly infected with malware that facilitated the breach and allowed hackers to “skim” the personal information. Barnes seeks certification of a “California class” of consumers whose personal information was compromised in the breach, with one of the questions of commonality asserted by Barnes to be determined as whether Hanna Andersson and Salesforce violated the CCPA by failing to maintain reasonable security procedures and practices. We expect to see several more cases like *Barnes* in the coming weeks and months.

**Conclusion**

Contact the authors and the other attorneys in the Data Security and Privacy team at Atkinson Andelson Loya Ruud & Romo to help you navigate the very complex regulations of the CCPA and ensure your business is ready and CCPA-compliant. If your business is faced with a lawsuit or regulatory enforcement under the CCPA, AALRR has a team of data privacy litigators well-versed in the CCPA and related law ready to step in and defend you.

The authors will also be presenting on the CCPA at the firm’s annual Employment Law Conference on March 26, 2020. If you are interested in attending, you may register online here.

This AALRR publication is intended for informational purposes only and should not be relied upon in reaching a conclusion in a particular area of law. Applicability of the legal principles discussed may differ substantially in individual situations. Receipt of this or any other AALRR presentation does not create an attorney-client relationship. The Firm is not responsible for inadvertent errors that may occur in the publishing process.

© 2020 Atkinson, Andelson, Loya, Ruud & Romo

**Tags:** California Consumer Privacy Act (CCPA), CCPA, Litigation, privacy