LOEB & LOEB LLP

Privacy

JANUARY 2, 2020

CCPA: A Spotlight on the Litigation Risks

After months of preparation, the effective date of the California Consumer Privacy Act (CCPA) is here. While there are a number of open questions about how the law will be interpreted, many companies are also struggling to understand how it will be enforced. Below are some of the potential claims companies might expect to see.

Key Takeaways:

- While the CCPA's primary enforcement mechanism is Attorney General (AG) enforcement, the CCPA does confer a private right of action in the event of data breaches, so data breaches present the most obvious risk of private litigation. Companies should review their security practices, benchmarking against industry standards to help demonstrate that their procedures are reasonable.
- Plaintiffs' attorneys may look to the Unfair Competition Law (UCL) and other California consumer protection statutes to bring class actions and other private litigations based on CCPA violations, including outside of the data breach context. Companies can try to deter such actions by clearly explaining their approach to compliance and aligning that approach to the expectations outlined in the AG guidance. Where the law is ambiguous, benchmark against others in your industry in an effort to stay within the pack.
- Companies should be prepared for nuisance requests under the CCPA from plaintiffs who are “fishing” for CCPA violations. Implementing an effective individual rights response program will help mitigate the risk from these requests.

California AG Enforcement

Violations of the CCPA are subject to enforcement by California's Office of the Attorney General. The AG can seek civil penalties of $2,500 for each violation or $7,500 for each intentional violation, after notice and a 30-day opportunity to cure have been provided. Enforcement proceedings will be delayed until July 1, 2020, six months after the CCPA goes into effect. California Attorney General Xavier Becerra has suggested, however, that he may bring retroactive enforcements for violations that occur between Jan. 1, 2020, and July 1, 2020.

Data Breaches Open the Door to Private CCPA Class Actions

The CCPA does not provide a general private right of action. It does confer a private right of action for claims arising out of a data breach, however. Specifically, consumers may sue a company for unauthorized access and disclosure of nonencrypted or nonredacted personal information resulting from the company's failure to implement and maintain reasonable security procedures and practices. For these violations, consumers may seek statutory damages ranging from $100 to $750 per incident, or actual damages.

This publication may constitute “Attorney Advertising” under the New York Rules of Professional Conduct and under the law of other jurisdictions.

The CCPA provides some relief to businesses in the form of a safe harbor, which requires consumers to first give the company written notice of the breach and 30 days to cure. While the CCPA does not explain how a company may cure a breach – leaving some ambiguity as to whether a cure has been effected – consumers may not seek statutory damages where a cure is effected within the safe harbor's 30-day cure period.

Plaintiffs' Attorneys May Also Attempt to Bring Class Actions Based on Non-Data Breach Violations of the CCPA

The CCPA gives consumers certain new personal information rights. A consumer may:

- Request information about a company's data collection and sales practices with respect to that consumer's personal information, including the categories of information collected, the source of the information, the use of the information, and what information was disclosed or sold to third parties.
- Request a copy of the specific personal information that a company collected about the consumer in the previous 12 months.
- Request (with certain exceptions) that a company delete the consumer's personal information.
- Request that a company not "sell" the consumer's personal information to third parties.
- Not be discriminated against by a company for exercising these rights.

Private plaintiffs' attorneys may work with consumers to make these requests and then file suit based on purported deficiencies in the response. Plaintiffs' attorneys might also claim deficiencies in "do not sell" mechanisms of companies as additional purported grounds for suit.

While the CCPA does not confer a private right of action for these types of violations, plaintiffs' attorneys have historically relied on such statutory violations to assert claims under other California consumer protection statutes, such as the California UCL, California's false advertising law and the Consumer Legal Remedies Act. In any such cases, plaintiffs' attorneys will have to overcome the CCPA's provision stating that "[n]othing in this title shall be interpreted to serve as the basis for a private right of action under any other law," a provision that is certain to be tested if plaintiffs' attorneys rely on CCPA violations as grounds to assert claims pursuant to other California statutes.

Another issue likely to arise in private actions brought in federal court is whether consumers have standing to assert claims for alleged privacy violations under the CCPA. The Supreme Court made clear in its 2016 decision in *Spokeo, Inc. v. Robins* that a statutory violation alone does not establish actual injury. Instead, plaintiffs must show some particular and concrete injury that resulted from the defendant's conduct. Courts have split on how to apply these standards in the data privacy context, but recent case law out of the Ninth Circuit indicates that violations of data privacy statutes may be sufficient to establish standing in California. Whether this applies to violations of the CCPA specifically is likely to be hotly contested.

California Cities and Counties Could Also Bring UCL Claims Based on Alleged CCPA Violations

California district attorneys representing cities and counties may also file UCL actions. Unlike private litigants, municipalities may recover up to $2,500 per violation in civil penalties. A recent California Court of Appeals decision held that district attorneys could not pursue state-wide UCL actions, reducing potential exposure for companies, but an appeal of that decision is currently pending before the California

Supreme Court. Regardless of the outcome of that appeal, larger municipalities in California have in recent years shown an interest in targeting data collection and sharing and may seek to enforce violations of the CCPA.

Where Do We Go From Here?

The risk of a private claim for a security breach will depend, in part, on whether a company's security practices are considered "reasonable." Companies should review their security practices, using as benchmarks industry standards as the Center for Internet Security's 20 Controls & Resources or the NIST Cybersecurity Framework.

Companies can try to deter private litigation (and subsequent Attorney General enforcement) by bringing their practices into compliance with the most widely accepted interpretations of the CCPA. Businesses should look to benchmark their approach against that of others in their industry. Staying in the middle of the pack, rather than testing the waters, may provide some comfort for companies looking to mitigate their litigation risk.

Finally, companies should continue to monitor statements from the AG's office regarding potential changes to regulations and interpretations of the law as well as enforcement priorities, and should be prepared to adapt quickly to changing guidance.

Related Professionals

For more information, please contact:

Jessica B. Lee	jblee@loeb.com
Wook Hwang	whwang@loeb.com
Susan E. Israel	sisrael@loeb.com
William Grosswendt	wgrosswendt@loeb.com

This alert is a publication of Loeb & Loeb and is intended to provide information on recent legal developments. This alert does not create or continue an attorney client relationship nor should it be construed as legal advice or an opinion on specific situations.

6161 REV1 01-08-2020