PUBLICATION

Recent CCPA Decision Portends Potential Expansion of Class Action Liability Exposure For Cookies, Pixels, and Tracking Technologies

Authors: David J. Oberly, Matthew George White, Aldo M. Leiva, Alexander Frank Koskey, III
May 02, 2025

Wild, wild, west? Web tracking may be the new frontier in class action litigation. With thousands of lawsuits filed in California and increasingly in other states against organizations, including many who may not realize the "long arm of the law" in these cases. In *Shah v. Capital One Financial Corp.*, No. 24 CV 5985, 2025 WL 714252 (N.D. Cal. Mar. 3, 2025), a California federal court took a broad view of the California Consumer Privacy Act's (CCPA) limited private right of action. The court allowed a CCPA claim to proceed past the motion to dismiss stage based on allegations that the Company intentionally disclosed personal information to third parties via web tracking technologies – despite the absence of a traditional data breach.

The *Shah* decision is notable, as it signals a potential broadening of the CCPA's private right of action – which allows for the recovery of statutory damages ranging between $100 and $750 per violation – beyond data breaches to unauthorized, non-breach disclosures involving the use of now-ubiquitous tracking technologies.

Background

While enforcement of the CCPA rests predominantly in the hands of the California Office of the Attorney General and the California Privacy Protection Agency (CPPA), the law also provides a limited private right of action under Cal. Civ. Code § 1798.150(a)(1) for any "consumer whose 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." In other words, to state a claim under the CCPA, a plaintiff must allege that his or her personal information was accessed 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.

Shah v. Capital One Financial Corp.

In *Shah*, credit card customers and applicants brought a putative class action lawsuit against the Company, alleging it violated (among other things) the CCPA by allowing third parties to embed tracking technologies on its website that transmitted their personal information to those third parties, which then used the data to target the plaintiffs with marketing advertisements.

The Company moved to dismiss, arguing that the plaintiffs' CCPA claim failed as a matter of law because the alleged CCPA non-compliance did not arise from a data breach. Construing the CCPA broadly, the court rejected this argument. Because the plaintiffs alleged that the Company allowed third parties – such as Facebook, Google, and Microsoft – to embed trackers on its website that disclosed the plaintiffs' personal information, the court reasoned that the plaintiffs did not need to allege a data breach. Instead, the plaintiffs' allegations that the Company disclosed their personal information without their consent through its use of embedded web tracking tools were sufficient to state a CCPA claim and avoid dismissal at the pleading stage.

Analysis & Takeaways

Historically, courts limited the CCPA's private right of action to circumstances concerning traditional data breaches. As indicated above, however, courts have more recently broadened their interpretation of Cal. Civ. Code § 1798.150(a)(1) to include intentional disclosures of consumers' personal information to third parties without their consent through tracking technologies.

For example, in *M.G. v. Therapymatch, Inc.*, No. 23 CV 4422, 2024 WL 421992, at *7 (N.D. Cal. Sept. 16, 2024), the court denied a motion to dismiss a CCPA claim where the plaintiff did not allege a data breach, but instead alleged the defendants disclosed his personal information without his consent through embedded Google Analytics code on its website. Similarly, in *Ramos v. Wells Fargo Bank, N.A.,* No. 23 CV 757, 2023 WL 5310540, at *2 (S.D. Cal. Aug. 17, 2023), the court held that the plaintiff stated an actionable CCPA claim, notwithstanding a failure to allege a data breach, where the plaintiff alleged "unknown individuals accessed information regarding his savings account as a result of Defendant's failure to properly maintain Plaintiff's nonredacted and nonencrypted information." Likewise, in *Stasi v. Inmediata Health Grp. Corp.*, 501 F. Supp. 3d 898, 924 (S.D. Cal. 2020), the court held the plaintiffs stated an actionable CCPA claim where they alleged their personal information was accessible over the Internet, but there was no theft.

Shah represents a continuation of the trend of courts seizing on the term "disclosure" in § 1798.150(a)(1) to permit CCPA class action claims involving the unauthorized disclosure of personal information through third-party tracking technologies embedded in a defendant's website.

Today, the practice of using third-party cookies, pixels, and other tracking technologies is ubiquitous across virtually all industries and sectors, including in many instances by companies who do not know – or do not fully understand – their practices. As a result, the potential expansion of the CCPA's private right of action – represented by *Shah* – beyond traditional data breaches poses a real risk of opening the floodgates to class action claims against all businesses that maintain any type of online presence in connection with their use of web tracking tools. Because the CCPA provides for the recovery of statutory damages ranging between $100 to $750 per violation – without any requirement to show actual harm or injury – the scope of potential liability exposure for CCPA non-compliance arising from web tracking tools is substantial.

What to Do Now

There are lessons to be learned from *Shah*. In today's digital landscape, companies with an online presence face a growing wave of class action exposure tied to the routine use of cookies, pixels, and other common web tracking tools. Several strategic measures – integrated into comprehensive compliance programs – can directly address and mitigate these risks and associated liability exposure arising from the high volume of tracking technology-related class action filings that will only increase for the foreseeable future.

Practical best practices include:

1. Assess website and mobile tracking tools and technologies.

Today, it is common for companies to deploy tracking tools, such as cookies and pixels, on their websites – without broader business or legal teams being fully aware. In many instances, only a few individuals in marketing have working knowledge as to the extent to which these tools have been deployed.

As illustrated by *Shah* (and in the proliferation of litigation challenging these technologies under state wiretapping laws), doing so comes with considerable risk. As such, companies should take proactive steps to assess their website and mobile tracking tools to evaluate the scope of personal data that is being collected and shared. In so doing, companies can gain a critical understanding of their websites' data practices, rather than discovering them for the first time only after receiving a demand letter or being named as a defendant in a class action complaint.

In particular, companies should closely assess what personal data is being shared with third parties through its use of tracking tools, and the necessity of and purposes for such disclosures. This is especially critical, as third-party data sharing practices have come under particularly heightened scrutiny by both enterprising plaintiff's class action attorneys and state and federal privacy regulators.

2. Update privacy policies and related external-facing privacy disclosures.

Companies should ensure their privacy policies and related disclosures clearly and conspicuously disclose all online analytics, marketing, and tracking tools that operate on their websites and other online properties. These disclosures should also identify and describe any related technologies or practices that may implicate the collection, use, or disclosure of visitors' personal data; for example, the use of session replay tools or data collected through the deployment of video content.

3. Maintain effective consent and opt-out mechanisms.

Companies should also ensure that they present their privacy policies to website visitors in a clear and conspicuous manner that, at a minimum, puts them on inquiry or constructive notice of their disclosures.

Whenever feasible, companies should consider implementing clickwrap consent mechanisms, which require users to click an "I agree" or similar button after being presented with a privacy policy link to signify their assent, as courts regularly uphold their validity. Importantly, companies should also conduct pre-deployment testing of their clickwraps to ensure that none of their tracking technologies "fire" until users affirmatively manifest their consent.

At the same time, in light of these recent decisions companies must also remain cognizant of the CCPA's opt-out requirements pertaining to the sale and sharing of personal information (as those terms are defined in California's consumer privacy statute).

The Final Word

In a world where tracking technologies are everywhere, ignoring privacy risks isn't an option. Companies must stay vigilant, especially as they navigate the tangled web of consumer privacy, wiretapping, and related laws – which are not only growing but often conflict with one another. Success requires more than good intentions; it demands a strategic, informed approach. Partnering with experienced outside privacy counsel is critical to building strong compliance programs that reduce the risk of becoming the next target in a privacy class action or enforcement action.

Our deep bench of Data Protection, Privacy and Cybersecurity professionals regularly counsel companies large and small on compliance and risk management strategies pertaining to the CCPA, the California Invasion of Privacy Act (CIPA), and numerous other consumer privacy, wiretapping, online marketing and advertising, and related laws. We also frequently provide guidance to companies across all industries on a range of other website and online privacy matters, including the development of enforceable online clickwrap and browsewrap agreements. At the same time, our Data Protection, Privacy and Cybersecurity Team closely tracks and monitors new privacy and technology legislative, regulatory, and litigation developments, as well as emerging trends.

For more information or assistance with CCPA compliance, or any related privacy or technology matters, please contact David J. Oberly, Matthew G. White, AIGP, CIPP/US, CIPP/E, CIPT, CIPM, PCIP, Aldo M. Leiva, Alexander F. Koskey, CIPP/US, CIPP/E, PCIP, or another member of Baker Donelson's Data Protection, Privacy Cybersecurity Team.