CLIENT ALERTS & INSIGHTS

Tracking Technology Trouble: Shah v. Capital One Deepens Legal Risk Under CCPA and CIPA

MAY 1, 2025

Authors: Adriana Beach

In Shah v. Capital One Financial Corporation, the Northern District of California handed down a ruling that may shape the trajectory of litigation involving tracking technologies, online privacy policies, and California's evolving privacy statutes, namely, the California Consumer Privacy Act ("CCPA"). The case is one of the latest in a growing line of digital privacy disputes premised on allegations that companies are disclosing personal and sensitive information to third- and fourth-party advertisers without consumer consent. Tracking technology trouble-now try saying that five times fast. But that isn't the only challenge here. This case highlights how courts are increasingly scrutinizing embedded tracking technologies under a broader interpretation of privacy statutes like the CCPA and CIPA.

The plaintiffs-a group of Capital One customers and credit card applicants-alleged that the financial institution used third-party trackers (including the Meta Pixel, Google, and Tealium) on its website to transmit sensitive data to advertising platforms. This included not just browsing behavior, but also financial details, such as credit card eligibility and employment information. The plaintiffs brought a sweeping 17-count complaint, asserting claims under both federal and California privacy laws as well as common law causes of action, such as breach of contract. Plaintiffs were given leave to amend most, though not all, of the dismissed claims.

Claims Asserted

The court's March 2025 decision granted in part and denied in part Capital One's motion to dismiss, resulting in a road map of what may-and may not-survive in similar litigation:

- **Negligence Survives, Negligence Per Se Does Not.** The court allowed the negligence claim to proceed, finding that the plaintiffs adequately alleged a duty of care in handling sensitive information. Notably, the court rejected Capital One's economic loss doctrine argument because plaintiffs claimed non-economic harms, such as time spent mitigating misuse. However, the court dismissed the negligence per se claim as not independently actionable under California law.
- **Claims Rejected Under Customer Records Act ("CRA"), Stored Communications Act ("SCA"), and Computer Fraud and Abuse Act ("CFAA").** The court dismissed claims under the CRA, finding Capital One exempt as a financial institution under the Gramm-Leach-Bliley Act. Claims under the SCA and CFAA also failed, the former because Capital One is not an "electronic communication service" and the latter due to insufficient pleading of the $5,000 statutory damage threshold.

- **A Partial Win on Common Law Claims.** While the court found that unjust enrichment claims could proceed, it dismissed claims for breach of express and implied contract, breach of confidence, and bailment.

Of particular importance was the court's decision on the plaintiffs' claims under the CCPA's privacy right of action, the California Invasion of Privacy Act ("CIPA"), and the Electronic Communications Privacy Act ("ECPA").

CCPA Claims

The Plaintiffs alleged that Capital One knowingly collected, used, and sold their personal information to third and fourth parties without consent. The court found these allegations sufficient at the pleading stage, particularly in light of the CCPA's requirement that a covered business provide consumers with notice of and the opportunity to opt out of certain disclosures of personal information with third parties.

Notably, the court adopted the reasoning in *M.G. v. Therapymatch, Inc., No. 23-cv-04422-AMO, 2024 WL 4219992, at *7 (N.D. Cal. Sept. 16, 2024),* which departed from the traditional understanding of a "data breach". Instead of requiring theft or exfiltration, the court concluded that allowing third-party trackers to access and transmit personal information without consent could constitute a data breach under the CCPA's private right of action. Specifically, the court found that "[b]ecause Plaintiffs' allege that Defendant allowed third parties to embed trackers, such as Google and Microsoft, on its website and that these trackers transmitted Plaintiffs' personal information," their claims were sufficient under the CCPA.

Importantly, this decision reaffirms that the scope of the CCPA's private right of action extends beyond traditional data breaches and includes online advertising ecosystems where data flows are often opaque to consumers. Consequently, it underscores the need for companies to maintain robust, transparent practices regarding data sharing and tracking-especially where sensitive personal or financial data is involved.

CIPA Claims

The Court also allowed plaintiffs' claims under both sections 631 and 632 of CIPA to proceed. These provisions address the unauthorized interception and recording of electronic communications, and the decision further clarifies how CIPA may apply to tracking technologies, respectively.

Under § 631, the court found that the plaintiffs plausibly alleged that Capital One used embedded trackers to intercept and transmit communications in transit without consent. The court rejected Capital One's argument that its privacy policy established consent, emphasizing that whether consent was given is a factual question not suitable for dismissal at the pleading stage.

Similarly, under § 632, the court held that allegations of tracking confidential communications, including application information and personal identifiers, via tools like the Meta Pixel were sufficient to proceed. The court reiterated that whether these communications were confidential and whether consumers had knowledge or consent would be determined later in the case.

Together, this demonstrates that companies deploying session recording or third-party marketing tools without clear, affirmative consent may find themselves vulnerable to liability under the CIPA. Notwithstanding, as this case foreshadows, expect additional litigation and judicial guidance as the legal definition of "consent" continues to evolve in this space.

ECPA Claims

The court also denied Capital One's motion to dismiss plaintiffs' claims under ECPA, holding that plaintiffs plausibly alleged an unlawful interception of electronic communications via Capital One's use of embedded tracking technologies-such as the Meta Pixel and Google Analytics-that captured the contents of consumers' communications in real time and transmitted them to third parties without authorization. Although Capital One argued that its role as a party to the communication exempted it under ECPA's one-party consent rule, the court rejected this defense-emphasizing that the alleged interception served a commercial purpose that violated privacy laws (i.e., the allegations that Capital One exploited consumers' interaction to target advertising and share sensitive and personal data without consent). This ruling aligns with recent case law holding that the one-party consent exemption does not apply where the interception is used to commit a violation of law, such as disclosing personal financial data to third-party advertisers without appropriate notice or consent. The decision also reinforces that ECPA, like CIPA, may be leveraged in session replay and tracking pixel litigation where companies use consumer communications beyond their original purpose and without adequate notice.

Looking Ahead

Shah underscores that even while providing consumers notice, and absent a traditional data breach or wiretapping, plaintiffs may successfully state claims based on data disclosures through embedded tracking technologies under various data privacy laws. Moreover, this case highlights how courts are increasingly scrutinizing tracking technologies-especially when evaluating privacy disclosures, the validity of consent, and what qualifies as harm under today's privacy laws.

Examine Notice & Consent. Companies should reexamine whether their privacy policies (and other applicable notices) adequately disclose the nature and scope of third-party data sharing-and whether consent mechanisms truly align with how information about consumers is being used in practice.

Conduct an Inventory of Website Trackers. Companies should identify and catalog all tracking technologies operating on their websites-including third-party pixels, cookies, session replay scripts, SDKs, and any embedded tools that facilitate behavioral analytics, targeted advertising, or mapping consumers' activities. This inventory should cover not only what technologies are present, but also what data they collect, how that data is shared, and with whom. Simply listing vendors is not enough-companies should evaluate whether each tool is configured to limit unnecessary data collection, and whether the associated third parties qualify as "service providers" or "contractors" under the CCPA or "processors" under other applicable privacy laws.

Review Contracts. Once tracking technologies are identified, companies review their contracts governing those tools-particularly with advertising platforms, analytics providers, and other data ecosystem participants. Companies should assess whether current agreements (including vendor

agreements, DPAs, and even click-through terms of use) permit these third or fourth parties to collect and use information about consumers beyond the scope of the service being provided. If these parties are leveraging the data for independent advertising or cross-context behavioral tracking, the company may not be able to classify these third (and fourth) parties as a "service provider" or a "processor" under applicable data privacy laws. That distinction can materially affect liability exposure.

Review Opt-Out Mechanisms and Global Privacy Controls. Many companies rely on passive disclosures or link-based opt-outs, but enforcement bodies and plaintiffs are increasingly scrutinizing whether those options are truly accessible, actionable, and compliant. Companies should confirm that consumers can exercise their rights across all devices and browsers and evaluate how Global Privacy Control (GPC) signals are honored across domains. Implementing a scalable, consumer-centric preference framework isn't just good hygiene-it could be central to a litigation or regulatory defense.

Monitor Proposed Legislation: Senate Bill 690. Companies should become familiar with pending legislation to modernize CIPA. Significantly, California Senate Bill 690, introduced in 2025, would exempt online technologies used for a "commercial purpose" from CIPA's wiretapping and pen register/trap-and-trace prohibitions and liability. If enacted, this amendment would significantly narrow legal exposure for businesses currently facing litigation risk for using internet-based communications and modern tracking tools in the ordinary course of business, such as chatbots, tracking pixels, and session replay technology. The latest version of the bill can be found here.

Adriana Beach is Of Counsel in Benesch's Data Privacy & Cybersecurity Practice Group. She can be reached at 628.295.2016 or abeach@beneschlaw.com.