Year in Review: 2023 Web Tracking Litigation and Enforcement

FEBRUARY 2, 2024

This post is part of a series of articles we are doing on 2023 data protection litigation trends. To stay up to date with our writings, please subscribe to the WilmerHale Privacy and Cybersecurity Blog.

2023 saw a rise in class action litigation related to internet tracking technology employed by companies to enhance user experience. Web tools like pixel systems, chatbots, and session replay software are used by company websites to collect and analyze user activity. Plaintiffs allege in these cases, for example, that personal data was collected, shared with third parties, and monetized for targeted advertising, allegedly all without user consent. Most of these class action lawsuits were brought in California, taking advantage of various wiretapping and anti-hacking statutes in the state. Although some of these claims have made it past the motion to dismiss phase of litigation, whether these cases will ultimately be successful remains to be seen; there are substantial hurdles that will need to be met before these cases proceed (along with substantial defenses under all the relevant legal claims).

Companies use various web tracking systems to collect consumer data and optimize user experience on their websites. Pixel systems and session replay software are common web tracking devices at issue in these lawsuits. A pixel is an invisible snippet of code embedded in a website that tracks user activity. Session replay software records user interaction with a website and creates a reproduction of the user experience for the website host. These tracking systems can record data such as clicks, pages visited, keystrokes, scrolls, and information entered into forms. Also, trackers may collect user-specific data, such as IP address, location, operating system, or browser type, typically used for targeted advertising. These tracking systems are often developed by third-party vendors and sold or provided to companies for installation on their websites. In addition to these web tracking tools, companies are also increasingly offering chatbots to users to help personalize their experiences. A chatbot is a computer program installed on websites that simulates human conversation with users, often for customer service purposes. These technologies have been used routinely by companies in virtually all industries to improve how the websites function and assist users in utilizing the sites.

The class action cases implicating these web tools raise a variety of legal theories and claims. Common law claims recurring in most web tracking lawsuits include breach of contract, invasion of privacy, and larceny. Alleged violations of various California statutes are also common in these lawsuits, including the

California Invasion of Privacy Act (CIPA), Unfair Competition Law (UCL), Confidentiality of Medical Information Act (CMIA), and Comprehensive Computer Data Access and Fraud Act (CDAFA).

Courts have discussed that each lawsuit is fact-specific, and whether claims get past the motion to dismiss phase depends on allegations made by the plaintiff and factual support for the same. Courts have been grappling with similar questions, like whether data collected by tracking systems is the type of personal information these statutes are intended to protect. Courts are also split on whether vendors of tracking technology should be exempted from liability as merely an extension of website host companies. This is particularly discussed when the vendor provided the product but did not use any data for its own purposes.

On top of litigation risk, companies should also be aware that the use of web trackers is top of mind for regulators, including the Federal Trade Commission and the Department of Health and Human Services (as evidenced in this joint letter the agencies sent out last year). It is likely to continue to be an enforcement priority in 2024.

In the rest of this post, we provide an overview of the specific California laws that plaintiffs use to bring lawsuits against companies that utilize these types of web tools as well as a sampling of these cases. We are happy to answer any questions you may have about this trend.

I. California Statutes Involved in Web Tracking Class Action Litigation

a. California Invasion of Privacy Act

Most class action plaintiffs have included claims under Sections 631 and 632.7 of the California Invasion of Privacy Act. In order to receive damages under CIPA, a plaintiff must show that there was a violation of the privacy rights provided under the statute. No other separate showing of injury is required, and CIPA provides $5,000 of statutory damages for each violation of the statute.

> Liability under Section 631 of CIPA can be broken into four clauses:
>
> 1. where a person intentionally taps, or makes any unauthorized connection with, any telegraph or telephone wire, line, cable, or instrument;
>
> 2. where a person willfully, and without consent of all parties to the communication, reads, or attempts to read or to learn the contents of, a communication while it is in transit;
>
> 3. where a person uses, or attempts to use or communicate, any information obtained through clauses (1) and (2); and
>
> 4. where a person aids or conspires with any person or persons to do any of the acts or things mentioned above.

Courts have been clear that the first clause applies only to communications through telegraph or telephone wire and not to internet communications. It also does not apply to plaintiffs who accessed websites through a smartphone, which has been characterized by courts as using a phone as a computer, not as a telephone. For this reason, complaints that involve this type of website activity, rather than communicating via telephone, have been dismissed.

CIPA was designed to prevent unlawful eavesdropping. Therefore, the second clause of Section 631 contains a party exception. This exempts from liability a person who is a party to the communication at

issue because a party cannot eavesdrop on its own conversation. Some courts have granted defendants' 12(b)(6) motions to dismiss, determining the party exception applies to the third-party company providing the web tracking software. In these cases, courts characterize the third-party vendor as merely an extension of the website host's company. Additionally, some courts have applied the party exception because the third party does not access or use the data for their own purposes. Courts are split on whether use or nonuse of the data is decisive on the party exception issue.

Because of the barriers associated with the first and second clauses, litigants have sued companies under the fourth clause, alleging that the website hosts are assisting third-party technology companies in unlawful wiretapping. To succeed under the fourth clause against a website host company, a plaintiff must also adequately allege a violation of one of the first three clauses against the third-party company. Some plaintiffs have struggled to do so because of the same issues discussed above.

Litigants have also brought claims under Section 632.7, which prohibits a person from intercepting and recording a communication between two telephones. Again, this section requires that the communication be over the telephone. Therefore, in cases where individuals used smartphones to access websites, they were deemed to be using their phone as a computer rather than as a telephone. These types of claims have generally been dismissed.

b. Computer Data Access and Fraud Act

The Computer Data Access and Fraud Act is also known as California's Anti-Hacking Law. Under this statute, a person can be liable if they knowingly access a computer system or data without permission. Liability can also occur if the person uses the data to wrongfully control or obtain money, property, or data, or takes or copies that data without permission.

Courts disagree on how to define "without permission." In some cases, the fact that a plaintiff merely did not consent to access of their data does not rise to the level of liability under the CDAFA. These courts interpreted the term "without permission" to mean the defendant overcame technical or code barriers to accessing the information. In these cases, plaintiffs were unable to overcome a 12(b)(6) motion for this claim. Other times, courts took up a broader definition of "without permission" using a plain meaning approach, which allowed the claim to survive.

c. Unfair Competition Law

Litigants suing under California's Unfair Competition Law may run into issues with standing. The UCL grants standing when a person suffers an injury in fact and has lost money or property because of the defendant's unfair competition. Therefore, there must be a showing of economic injury caused by the unfair business practice. It is helpful to plaintiffs that the Ninth Circuit previously held that users' browsing history had a specific financial value. However, to survive a 12(b)(6) motion to dismiss, plaintiffs must allege specific factual allegations of the economic value of their data. In general, UCL claims do not appear to be successfully moving past the motion to dismiss phase in web tracking class action lawsuits

d. Confidentiality of Medical Information Act

The California Confidentiality of Medical Information Act prohibits the unauthorized disclosure and negligent preservation of medical information. Plaintiffs must claim their medical information was disclosed without consent and that it was improperly viewed or accessed. Some CMIA claims may survive the motion to dismiss phase if the pleading contains factual support for the plaintiff's belief that their data

was improperly viewed, like in *Doe v. Regents*, discussed below. Otherwise, assumptions that data was improperly accessed will likely cause a CMIA claim to be dismissed.

II. Example Cases

a. Healthcare Entities

Many cases involving healthcare entities concern pixel systems installed on these entities' websites and patient portals. Plaintiffs complain that these pixels collect sensitive patient information and then transmit that personal health information to the third-party vendor that provides the pixel technology, without patient consent.

In *Cousin v. Sharp Healthcare*, plaintiffs alleged that Sharp Healthcare disclosed patient health information through a pixel tracking tool on its website. The plaintiffs' complaint included five causes of action: (1) breach of fiduciary duty; (2) violation of common law privacy intrusion against seclusion; (3) invasion of privacy under the California Constitution; (4) violation of CMIA; and (5) violation of CIPA.

In this case, the court discussed some of the issues with the plaintiffs' complaint, including that the complaint was missing factual support for plaintiffs' contention that their personal information was disclosed. In addition, the court questioned whether data about researching doctors, looking for providers, and searching for medical specialists is considered protected health information. Because of these pleading defects, the court dismissed all claims. In this case, the court also addressed damages in regard to the plaintiffs' invasion of privacy claim and stated that California's constitutional provision protecting the right of privacy supports a cause of action for an injunction, but not a private right of damages.

In *Doe v. Regents of University of California*, the plaintiff made similar claims regarding use of pixel tracking. The plaintiff asserted that she entered data into her patient portal related to heart issues and high blood pressure and later received targeted advertisements related to her conditions on her social media, including one for high blood pressure medication. The plaintiff's CIPA claim was dismissed because the defendant is a public entity and therefore had immunity. However, the plaintiff's CMIA, common law intrusion against seclusion, and breach of implied contract claims all made it past the defendant's motion to dismiss. The court remarked that the plaintiff's allegation regarding the targeted advertising she saw provided plausible factual support for a CMIA claim. Additionally, when discussing the plaintiff's intrusion against seclusion claim, the court observed that personal medical information is some of the most sensitive information about an individual, suggesting that this data is the type that should be protected. In regard to damages, the court in Regents also determined that the plaintiff could only seek an injunction, not monetary damages, for claims falling under Article 1, Section 1, of the California Constitution.

b. Retail Companies

Chatbots are often used on retail company websites to allow customers to ask customer service questions. In *Swarts v. Home Depot*, a plaintiff alleged that Home Depot recorded his conversation with a chatbot without his consent, in violation of wiretap laws. Here, the plaintiff's claims included violations of CIPA, UCL, and the Wiretap Act. Because of the barriers discussed above with CIPA, the CIPA claims were dismissed with leave to amend. The plaintiff's UCL claim was dismissed with no ability to amend, because the court determined that the plaintiff could not meet the threshold requirements for UCL, including an economic injury.

Session replay software reproduces, for the website host, users' interactions on the website, including movements, clicks, page visits, scrolling, and keystrokes. Several class action lawsuits against retail companies involve the use of session replay. For example, in *Love v. Ladder Financial, Inc.*, plaintiffs sued both Ladder Financial (Ladder) and FullStory (the vendor of the session replay software), alleging that Ladder used FullStory's session replay tool to collect data in a way that constituted wiretapping. The plaintiffs alleged violations of CIPA and UCL, and invasion of privacy under the California Constitution. Both Ladder and FullStory filed motions to dismiss, which were both granted on January 11, 2024. The plaintiff has since filed an amended complaint against Ladder.

Authors

Kirk J. Nahra

PARTNER

Co-Chair, Artificial Intelligence Practice

Co-Chair, Cybersecurity and Privacy Practice

kirk.nahra@wilmerhale.com

+1 202 663 6128

Samantha J. Kanekuni

ASSOCIATE

samantha.kanekuni@wilmerhale.com

+1 202 663 6135

Ali A. Jessani

SENIOR ASSOCIATE

ali.jessani@wilmerhale.com

+1 202 663 6105