

Privacy Litigation Trends – Back to the Future

October 26, 2023 – *The TMCA*

by Austin T. Chambers and Deb Howitt

Plaintiffs look to the past to take action against modern web tracking

As states rapidly enact new consumer privacy legislation, businesses have been working tirelessly to comply with extensive new data protection obligations and build out compliance programs. Despite the fact that these new state laws lack a private right of action for violations associated with online tracking and data sharing, private plaintiffs across the country have found creative workarounds, filing a wide range of novel claims alleging violations of decades-old privacy laws. These claims seek to expand the reach of these older laws to modern technologies, adding a new, dynamic layer to businesses' privacy concerns.

Driving the explosion in litigation are a series of decisions that have given new life to claims under state and federal wiretap laws and for violation of state constitutional common law privacy rights in the context of common online technologies. As a result, private plaintiffs are increasingly bypassing the broad limitations on private rights of action common to state consumer privacy laws, and making demands that go beyond, or potentially conflict, with the requirements set out in those laws.

For now, many of these actions are relatively novel claims working through lower courts, often on preliminary motions. The causes of action and defenses continue to evolve, and there remains considerable change and uncertainty as these cases develop. However, recent trends suggest that courts are engaging in critical and nuanced evaluations of these claims in the context of popular online advertising and communications technologies.

Related People

- Austin T. Chambers

Related Capabilities

- Trademark, Copyright + Advertising
- Intellectual Property Litigation



What technologies are the focus of Plaintiffs' claims?

The key technologies at issue in these cases are online advertising services, social media “pixels,” “chatbots,” and “session-replay” technologies commonly used by businesses with consumer-facing online services.

- **Online advertising**, such as display advertising, retargeting, or remarketing services often involve the use of consumer profiles that are accessed and distributed among myriad companies involved in the ad personalization and bidding process.
- **Social media pixels and other integrations** allow companies to connect their website with social media services to obtain insights about consumer demographics and other marketing data and to run targeted marketing campaigns on popular social media sites.
- **Chatbots** are third party tools that companies add to their sites that allow customers to seek support, find products, and ask questions.
- **Session replay** technologies involve the recording of user interactions on sites for usage, debugging, and similar analytical purposes, but which may involve creating a record of user data entered in form fields, or similar information.

In each case, third party providers operate these technologies and are granted access to data relating to the customer’s activity on and other interactions with the business’s online services and, in some cases, communications with the business. In the case of social media pixels, social media companies may have access to information such as the products or content that the user viewed, shopping carts, purchases, and other information revealed by ‘tags’ that companies place on their services. Social media sites then link this information to a user’s social media profile or other information the platform holds about the user, which the business can then use to obtain insights about consumer behavior and to target advertising to similar users on social media sites.

What claims are plaintiffs bringing?

To challenge companies' use of these technologies, plaintiffs are looking to the past, bringing challenges under state and federal wiretap acts (telephone privacy), under state constitutional or common law privacy (e.g., invasion of privacy, intrusion upon seclusion), and the Video Privacy Protection Act ("VPPA"), a relatively obscure 1987 law passed in response to the disclosure of supreme court nominee Robert Bork's video rental history. Each of these laws permit private claims and provide for statutory damages, which may allow private individuals to bring claims without proof of actual damages.

The federal Wiretap Act (18 USC § 2511) provides a cause of action against "any person who ... intentionally intercepts ... or **procures any other person** to intercept or endeavor to intercept any wire, oral or **electronic communication**." Similarly, California's Invasion of Privacy Act (Cal. Pen. Code § 631(a)) "CIPA") provides a cause of action against a person who "attempts to read, or to learn the contents or meaning of any message, report, or **communication**" including anyone "who **aids, agrees with, employs, or conspires with any person** or persons" to engage in such conduct. However, both CIPA and the federal wiretap act allow such conduct with the consent of all parties to the communication.

In addition to the wiretap claims, plaintiffs have brought claims under state constitutional or common law for invasion of privacy. For example, in California a person has a cause of action where another person 'intentionally intrudes into a place, conversation, or matter as to which the person has a **reasonable expectation of privacy** and the intrusion is **highly offensive** to a reasonable person.'

The VPPA (18 USC § 2710) provides a cause of action against a "**video tape service provider** who knowingly discloses, to any person, **personally identifiable information** concerning any **consumer** of such provider" without authorization. While the VPPA was originally intended to address videotape rental services, the VPPA also applies to "any person engaged in the business ... or deliver or prerecorded video ... tapes or similar audio visual material."

For each of these claims, plaintiffs fundamentally allege that behavioral and interaction data collected by online services reveals private information, communications, or other information protected by law. For example, in cases where defendants use online advertising or social media pixels, plaintiffs allege that these services allow the website operators, or their advertisers or social media partners, to collect detailed, private information relating to their demographics, preferences, and behaviors. For businesses with video offerings, plaintiffs further allege that the disclosure of information relating to the videos, e.g., the title, violates the VPPA. Similarly, on sites that use chatbots or session replay technologies, plaintiffs often allege these technologies result in the disclosure of protected communications.

The outcome of these claims tend to turn on several of key facts:

In all cases:

Did the plaintiff provide consent?

- The quintessential defense to each of these claims is the plaintiff's consent to the collection or disclosure of the information at issue. However, there remains some dispute over the elements of consent required in each case. Important open questions include the means and extent to which a plaintiff was notified of the alleged conduct (e.g., via a standalone notice or general privacy policy), or whether the plaintiff affirmatively opted-in, acknowledged the use, or if legal notices were available for review when the plaintiff used a service.

Was there actual harm?

- Despite statutory damage provisions, there remain open questions as to whether plaintiffs can bring claims in cases where there is no injury in fact or no allegation of legally cognizable harms. The Supreme Court's landmark *Spokeo* and *TransUnion* cases continue to develop alongside many of these claims.

For wiretap claims:

Does the technology involve the disclosure of communications content?

- Generally, wiretap claims require the defendant to have intercepted the *content* of a communication, not merely information *relating to* the communication (e.g., number dialed, time, etc.). Wiretap laws such as CIPA also cover interception of the *meaning* of a communication. In the case of behavioral advertising or social media, there is considerable debate as to whether browsing metadata that reveals demographic information, usage history, or information regarding products viewed or purchased reflects a "communication." Similarly, in cases of session replay technologies, it may be unclear whether actual communications, or mere interaction data were collected, especially where services offer redaction tools that enable operators to exclude communications content, but the redactions are not visible to the public (or in a manner sufficiently apparent at the pleading stage).

Is the party a third party?

- Where a defendant or their agent is a party to communication, those parties generally cannot be liable under wiretap laws. Therefore, in cases where a service provider is required to provide services only on behalf of a business (i.e., subject to a services agreement and data protection agreement), parties may be able to avoid liability and dismiss claims under wiretap acts under this exception. However, where social media companies or advertisers can use data for their own purposes, it is debatable (and highly context dependent) whether the social media platform could be deemed a party to the communication.

For invasion of privacy claims:

Does the plaintiff have a reasonable expectation of privacy?

- Foundational to all invasion of privacy claims is the defendant's reasonable expectation that the information or communication was private. As with wiretap cases,

where a business collects only general commercial information or metadata about a communication—but no actual communication—courts are less likely to find that the defendant has a reasonable expectation of privacy. Where the volume or nature of data reveals only common, or readily observable behavior, courts are also less likely to find a reasonable expectation of privacy. However, where a business collects detailed search histories or other data that collectively reflects the substance of a communication or significant amounts of information about a person, some courts have found that plaintiffs may have a reasonable expectation that such information would remain private. A defendant's conduct can also give rise to expectations of privacy, e.g., though the provision of opt-out options, or affirmative statements that certain data would not be collected.

Was the conduct highly offensive?

- In addition to the plaintiff's reasonable expectation of privacy, the defendant's conduct must be "highly offensive." There is considerable debate over this element, as courts often must consider vague, and sometimes evolving, social norms. However, in cases where information collected is general commercial information or otherwise non-sensitive, courts often find that such conduct was not offensive enough to support a claim, notwithstanding the plaintiff's reasonable belief that the information would remain private.

For VPPA claims:

Is the business a video tape service provider?

- The VPPA applies only to video tape service providers that are "engaged in the rental, sale, or delivery of prerecorded video cassette tape or similar audio visual materials." While courts have expanded this to online streaming services and other online video platforms, courts have found that a party may not be a "service provider" where they merely deliver video content (for no fee) or where the video offering is only ancillary to the business (e.g., a video on a marketing website for a consumer products company). Similarly, courts have found that providers offering live content or livestreams are not video service providers.

Is the plaintiff a "consumer"?

- A consumer for purposes of VPPA is a "renter, purchaser, or subscriber of goods or services from a video tape service provider." Recent VPPA cases have scrutinized the nexus between plaintiffs' relationships with the business and the video content at issue. In cases where video is neither core to the business nor the subscription or purchase transaction, courts have found that an individual is not a consumer for VPPA purposes. However, where exclusive video content or similar offerings are made to subscribers as part of a purchase, courts are more likely to find a sufficient nexus between the video content and a subscription or other commercial transaction.

Is the disclosed data "personally identifiable"?

- The VPPA defines personal information "as information that *identifies* a person as having requested specific video material from the video tape service provider." This definition is narrower than definitions under modern consumer privacy laws that extend to data that is identifiable or linked or linkable to a person. Some data from social media services is known to link directly to user profiles that readily identify

individuals, and as such may be personally identifiable. However, data that is not directly identifiable, such as anonymous user IDs (isolated from data sufficient to link to a known ID), IP addresses, and the like may not be personally identifiable for purposes of the VPPA.

How should businesses respond?

In response to the wave of cases, businesses should take steps to ensure that they review and evaluate the implementation of common web technologies, in particular those involving social media, advertising, session replay technologies, and video content. Dorsey's team of privacy lawyers can provide advice and assistance with measures to mitigate the risks of litigation under these novel claims.

Dorsey's privacy team will continue to monitor these cases and report on updates as courts consider these cases and critical facts continue to develop.