DAVIS GILBERT

Litigation + Dispute Resolution

Can you Wiretap a Website? Decades-Old Privacy Laws Are Being Used to Attack Common Internet Technologies

The Bottom Line

- Nearly any business with a public-facing website is susceptible to plaintiffs seeking to apply decades-old state privacy laws to modern and common online practices.
- Despite murky case law, there are some viable defenses that can be raised, including that the plaintiff does not have standing because there is no concrete harm.
- User consent to the use of tracking technologies may also be a defense, and, as a result, website operators and app providers should include strong disclosure and consent mechanisms to bolster their defenses.
- Potential statutory damages can quickly add up, particularly in threatened or putative class actions.

Privacy and wiretapping laws like California's Invasion of Privacy Act (CIPA), Massachusetts's Wiretap Act (MWA), and the federal Wiretap Act (FWA) were originally designed to prevent unwanted eavesdropping on telephone calls.

These laws, enacted before websites were ubiquitous or even known, have become hotbeds for individual and class action claims, both threatened and filed. Today, these laws are being leveraged against technologies that are at the heart of most website functionality, including the use of cookies, pixels, chatbots and other tools that can track a user's online activity.

Most websites employ such technologies to enhance consumers' interactions with their websites, generate analytics, deliver targeted advertising, and create consumer profiles. These statutes also provide relatively high statutory damages per alleged violation, and even potential criminal penalties. In an otherwise murky body of law, California and Massachusetts courts have recently limited the scope of these claims to be more aligned with related federal laws including the Video Privacy Protection Act (VPPA) and FWA.

CIPA Claims

CIPA (Cal. Penal Code § 630, *et seq*) claims generally fall into two categories, under Section 631(a)'s prohibition on wiretapping, and now increasingly under Section 638.51's prohibition on the installation and use of a pen register or trap and trace device. Either claim can be defeated if the plaintiff does not have standing.

Wiretapping Claims

Section 631(a), a corollary to the FWA, generally prohibits "wiretapping", which historically concerned the use of technology to listen in on telephone communications without the consent of the parties on the call. Plaintiffs are now using Section 631(a) under the statute's aiding and abetting provisions to assert claims against websites that have installed third-party technology to track or record consumer communications and interactions with the website.

A user's consent or authorization to such interception may be a defense to this claim, and, as a result, websites and apps are increasingly including consent management platforms (*e.g.*, a cookie consent banner when a user first visits a website) to bolster the defenses to such claims. However, some courts have allowed such claims to proceed, even despite evidence of consent.

Pen Register or Trap and Trace Device Claims

A new wave of claims draws on Section 638.51, which prohibits the "install[ation] or use [of] a pen register or a trap and trace device without first obtaining a court order" or consent, in certain circumstances. A pen register is defined as a device or process that records or decodes dialing, routing, addressing, or signaling information, but not the contents of a communication. A "trap and trace" device is defined as functionally similar, but it records the incoming numbers to a particular line, rather than the outgoing numbers that a pen register captures. Courts have been more mixed on whether consent is a complete bar to these claims.

California Court Holds Testers Lack Standing to Bring CIPA Claims

Regardless of the type of CIPA claim asserted, standing is a threshold defense. For example, in *Rodriguez v. Fountain9*, a recent decision from the Los Angeles County Superior Court concerning the use of tracking software on a website, the court held that alleging a strict statutory violation under CIPA without any concrete harm is insufficient to support standing. The court indicated that the plaintiff needed to allege something more, for example, "that Defendant is tracing Plaintiff's activities or is creating a digital fingerprint of Plaintiff."

Massachusetts Limits the Scope of its Wiretap Act

Massachusetts' highest court recently held in *Vita v. New England Baptist Hospital* that the MWA (M. G. L. c. 272, § 99) does not prohibit website operators from using tracking software. In *Vita*, the court rejected the plaintiff's claims that the MWA protects her from unwanted tracking and transmission to third parties of her interactions with her healthcare providers' websites. The court explained that although the statute does not expressly define "communication", "[b]ased on our review of the text of the wiretap act and its legislative history, we cannot conclude with any confidence that the Legislature intended 'communication' to extend so broadly as to criminalize the interception of web browsing and other such interactions." The court specifically focused on the fact that these interactions "are not with another person but with a website." Looking to the statute's plain text and legislative history, the court held that "communication" should be limited to conversations or messages between people and did not reasonably encompass the type of web "browsing and interacting" that the *Vita* plaintiff had engaged in, particularly considering the criminal penalties of fines, imprisonment, or a combination thereof, in addition to civil penalties including liquidated damages.

Related Federal Laws

Earlier this summer, in *Brown v. Learfield Commc'ns, LLC*, a federal court in Texas rejected a plaintiff's second proposed class action alleging that the University of Texas's use of Meta's Pixels on its website violated the FWA and VPPA by failing to disclose the tracking and sharing of personal identifying information and viewing history.

As to the FWA claim, like the *Vita* Court, the court held that the plaintiff failed to plausibly allege that the University of Texas "intercepted [the communications] for the purpose of committing any criminal or tortious act." Second, the court held that the University of Texas' website manager was considered a "party" under the FWA and so could not unlawfully intercept communications that users direct to their sites because they are, in effect, the intended recipients of those communications.

Litigation + Dispute Resolution

For More Information

Please contact the attorneys listed below or the Davis+Gilbert attorney with whom you have regular contact.

Gary Kibel

Partner
212 468 4918
gkibel@dglaw.com

Marc Rachman

Partner
212 468 4890
mrachman@dglaw.com

Sarah Benowich

Associate
212 468 4991
sbenowich@dglaw.com