Articles + Publications | November 12, 2024

Is AI Eavesdropping on You??

WRITTEN BY

Kenneth K. Suh | Emma Bennett

Consumer-facing artificial intelligence ("AI") tools are quickly becoming the target of wiretapping class actions, particularly in California where the state's wiretapping law provides for statutory damages and has been interpreted broadly by the courts. Businesses utilizing AI tools should carefully review their privacy policies, terms of use, and third-party provider agreements to ensure that they provide consumers clear disclosure regarding the use of AI tools and the potential use of a consumer's information or interaction with the company to further train AI tools.

Wiretapping laws go back to the 1960's and were primarily developed to curtail impermissible eavesdropping on, now thing of the past, landline phones. The term "wiretap" has literal meaning as landlines had to be physically compromised, *e.g.* tapped, in some way. It's hard to imagine that in 1967, the drafters of the California Invasion of Privacy Act ("CIPA"), California's wiretapping law, imagined the act could be applicable to advanced artificial intelligence over 50 years later.

While businesses have been utilizing AI tools to streamline ad and pixel tracking,[1] consumer-facing business applications are quickly emerging. For instance, companies utilize AI-powered chat bots in place of virtual customer service agents, AI chat bots are skimming customer reviews to provide answers to customer inquiries related to whether a product suits their needs, AI chat bots are aiding customers in returns and exchanges, AI voice assistants are answering customer service phone calls, and AI tools are now being used to take orders from customers. In a vast majority of these instances, businesses rely on a third-party service provider for the AI tool.

A flurry of lawsuits, in the wake of the ad and pixel tracking lawsuits, are hitting businesses with consumer-facing AI tools in California. These lawsuits allege that the third-party AI technology intercepts and records customer communications without their consent and subsequently, the third-party AI provider uses their communications to train the AI tools, all in violation of the California Invasion of Privacy Act.

I. California Invasion of Privacy Act

The California Invasion of Privacy Act (CIPA)[2] is a wiretapping law that prohibits recording confidential conversations without the consent of all parties. CIPA has three unique characteristics compared to the wiretapping laws of other states:

1. Requires the consent of all parties to a communication;
2. Has multiple causes of action, including one that courts interpret broadly to apply to internet-based communications and one specific to aiding and abetting someone else's eavesdropping; and
3. Provides for statutory damages of $5,000 per violation, plus attorneys' fees and costs.[3]

©2026 Troutman Pepper Locke

At the outset, CIPA states the intent is for the statute to evolve to accommodate developments in technology:

The Legislature hereby declares that advances in science and technology have led to the development of new devices and techniques for the purpose of eavesdropping upon private communications and that the invasion of privacy resulting from the continual and increasing use of such devices and techniques has created a serious threat to the free exercise of personal liberties and cannot be tolerated in a free and civilized society.[4]

Under § 631 of CIPA, California courts have narrowed down the liability to fall in four categories: (1) intentional wiretapping any telegraph wire, telephone wire or the like, (2) willfully attempting to learn the contents or meaning of a communication in transit over a wire, (3) attempting to use or communicate information obtained as a result of engaging in either of the two previous activities, or (4) aiding and abetting another to violate any of the other three categories.

Importantly, while the first cause of action specifically includes the phrase "any telegraph or telephone wire, line, cable, or instrument, including the wire, line, cable, or instrument of any internal telephonic communication system," the second cause of action only requires willfully attempting to learn the contents or meaning of a communication "over a wire." The aiding and abetting cause of action applies to any entity that helps another entity act in a way contrary to the first three causes of action.

Affirmative Defenses

CIPA includes three statutory defenses, each of which narrowly applies only to public utilities, telephone companies, and telephone systems within correctional facilities.[5]

However, a common defense to computer-based CIPA cases, including those involving AI tools, is the "Party Exemption" defense—where a party to the conversation cannot eavesdrop or wiretap its *own* conversation. Some California courts have found this exemption applicable in situations where a business uses a third-party service provider to communicate with consumers. In those decisions, courts have found that the third-party technology is merely a "tool" and acting as an extension of the company. However, courts apply this defense only when the agreement between the business and their third-party service provider clearly articulates that the service provider is acting directly and only on behalf of the business, and the service provider is not using the interaction with the customer for any other purpose.[6] However, where the third-party service provider collects, uses, and sells the data collected for its own use, rather than solely for the benefit of the business, the "Party Exemption" may be inapplicable.[7]

II. AI Chat Bots and Voice Assistants

In 2024, businesses using third party AI-powered chat bots and voice assistants have been the subject of several lawsuits under CIPA:

- In February 2024, a plaintiff brought a class action against The Home Depot and Google for The Home Depot's use of Google's Cloud Contact Center AI.[8] The plaintiff alleges that Google's AI software analyzes live customer calls in violation of CIPA § 631. On August 28, 2024, before either defendant filed an answer, the plaintiff voluntarily dismissed the action without prejudice. The plaintiff refiled the case just against Google in the Northern District of California on September 3, 2024.[9] The allegations mirror those from the first lawsuit and

allege Google's Cloud Contact Center AI violates CIPA. Google was scheduled to answer on November 5, 2024.

- In May 2024, another plaintiff brought a class action against Navy Federal Credit Union and their real-time customer care vendor, Verint.[10] The plaintiff alleges that the use of the Verint software violates CIPA §§ 631 and 632, is a violation of the right to privacy under California's Constitution, is an intrusion upon seclusion, and is a breach of the parties' quasi-contract. In response, the defendants jointly filed a motion to dismiss for lack of personal jurisdiction, improper venue, lack of standing, failure to state a claim, lack of proper service against Navy Federal Credit Union, and a request to transfer to the Eastern District of Virginia. In the motion to dismiss, the defendants assert the party exemption to the CIPA claims. On September 19, 2024, the plaintiff voluntarily dismissed the action without prejudice.
- In June 2024, another plaintiff brought a class action for Peloton's use of a third-party's, Drift, technology in its online chat, allegedly violating CIPA §§ 631 and 632.[11] Peloton moved to dismiss the complaint and argued that Drift's actions fall under the "Party Exemption" and that plaintiff only alleged actions under CIPA § 631 category (3). On July 5, 2024, the court denied Peloton's motion to dismiss and found that the plaintiff pled facts sufficient to satisfy category (2), along with category (3). Further, the court concluded that plaintiff sufficiently alleged that Drift's software uses Peloton's customer data for its own benefit and therefore the "Party Exemption" may not apply. Peloton then answered on August 2, 2024 and submitted standard affirmative defenses and specific CIPA defenses of 'consent' and 'no aiding and abetting.' On September 30, 2024, the parties jointly filed a voluntary dismissal, with prejudice as to plaintiff's claims.
- In July 2024, a plaintiff filed a putative class action in California state court against Patagonia based on its alleged use of customer service vendor Talkdesk's software.[12] The plaintiff alleges that Patagonia's use of the Talkdesk software violates CIPA §§ 631 and 632, is a violation of the right to privacy under California's Constitution, and is an intrusion upon seclusion. On October 24, 2024, the parties jointly filed a voluntary dismissal.

III. Lessons Related to Use of Customer-Facing AI Tools

It seems that AI is being implemented into every aspect of business operations, including consumer-facing applications. But before on-boarding a new third-party AI service provider, companies should consider whether the AI-tool is communicating directly with customers, which party retains the rights to the data related to the communications, and how that data may be used. Companies should be aware of, and understand the associated risks, related to how third-party AI service providers are collecting data, how the data is being used, whether the data is training the AI, whether the third party is using the data for any other internal purposes, and ensure that companies are, as needed, properly disclosing to consumers and receiving consent for these activities under CIPA and other privacy laws.

Appropriate and informed third party service provider management, along with robust external and internal privacy policies and procedures, can help guard against risks as businesses eagerly develop and release new AI-powered tools.

—

[1] There has been litigation about non-AI portions of ad and pixel tracking violating state wiretapping laws on a similar basis as the AI chat bots and AI voice assistants discussed herein. This litigation so far has resulted in favorable outcomes for the tracking software giants like Meta and Google. For example, on October 24, 2024, Massachusetts Supreme Court found that use of tracking software (Google Analytics and Meta Pixel) does not violate the state's wiretap law. *Vita v. New England Baptist Hospital et al.*, No. SJC-13542 (Mass. Oct. 24, 2024).

[2] Cal. Pen. Code §§ 630 *et seq.*

[3] *Id.* §§ 631; 632.

[4] *Id.* § 630.

[5] *Id.* §§ 631; 632.

[6] *Byars v. Hot Topic, Inc.*, 656 F. Supp. 3d 1051 (C.D. Cal. 2023); *Graham v. Noom*, Inc., 533 F. Supp. 3d 823 (N.D. Cal. 2021).

[7] *In re Facebook, Inc. Internet Tracking Litig*, 956 F.3d 589, 607 (9th Cir. 2020); *Esparza v. UAG Escondido AI Inc.*, 2024 WL 559241, at *7 (S.D. Cal. 2024).

[8] *Barulich v. The Home Depot, Inc. et al.*, No. 2:24-cv-1253 (C.D. Cal. Feb. 14, 2024).

[9] *Barulich v. Google, LLC.*, No. 3:24-cv-06225 (N.D. Cal, Sept. 3, 2024).

[10] *Paulino v. Navy Federal Credit Union et al.*, No. 3:24-cv-3298 (N.D. Cal. May 31,2024).

[11] *Jones v. Peloton Interactive, Inc.*, No. 3:23-cv-1082 (S.D. Cal. June 9, 2024).

[12] *Gills v. Patagonia, Inc.*, No. 2024CUNP026848 (Cal. Superior – Ventura July 11, 2024).

RELATED INDUSTRIES + PRACTICES

- Artificial Intelligence
- Privacy + Cyber