Cos. Must Address Growing Chatbot Class Action Risk

By **Melanie Conroy, Kathleen Hamann and Ariel Pardee** (November 2, 2023)

Melanie Conroy

Kathleen Hamann

Ariel Pardee

In a new wave of consumer data privacy litigation, plaintiffs have recently filed dozens of class actions in state and federal courts, primarily in California, seeking damages for alleged wiretapping by companies with public-facing websites.

The complaints assert a common theory: that website owners using chatbot functions — also known as artificial intelligence virtual assistants — to engage with customers are violating state wiretapping laws by recording chats and giving service providers that support those functions with access to them, which plaintiffs label illegal eavesdropping.

Chatbot wiretapping complaints seek substantial damages from defendants and assert new theories that would dramatically expand the application of state wiretapping laws to customer support functions on business websites.

Although there are compelling reasons why courts should decline to extend wiretapping liability to these contexts, early motions to dismiss these cases have met mixed results.

Therefore, businesses that use chatbot functions to support customers now face a high-risk litigation environment, with inconsistent court rulings to date and uncertain legal holdings ahead, significant statutory damages, and a rapid uptick in plaintiff activity.

States With the Strictest Wiretapping Laws

California and Massachusetts have some of the most restrictive wiretapping laws in the nation, applicable not only to law enforcement and governmental actors, but to private citizens and businesses as well.

Both states require all parties to consent to a recording, in contrast to the one-party consent required under federal law, and both states have privacy statutes that litigants have invoked to bring claims based on alleged wiretapping.

The Massachusetts Invasion of Privacy Act was enacted in 1968 and provides that each person "shall have a right against unreasonable, substantial or serious interference with his privacy."[1] This right to privacy extends to private communications, as encoded in the Massachusetts Wiretap Statute, which prohibits the unauthorized interception of wire and oral communications unless a recognized exemption applies.[2]

Massachusetts' wiretapping statute provides for a civil damages award of actual and punitive damages, not less than liquidated damages computed at the rate of $100 per day for each day of violation or $1,000, whichever is higher, plus attorney fees.[3]

Efforts to modernize these laws, including to update definitions to reference forms of

electronic communications that did not exist in 1968, have faltered despite strong support from former Massachusetts Gov. Charlie Baker and then-Attorney General Maura Healy.[4] Nonetheless, litigants have sustained claims past the pleading stages, alleging that MIPA applies to the recording of website activity in recent session-replay suits.[5]

In those cases, plaintiffs have sought damages for invasion of privacy under MIPA based on alleged violations of wiretapping laws through the interception and disclosure of website communications and activity.

The California Invasion of Privacy Act was enacted in 1967, and prohibits wiretapping and eavesdropping upon private communications with limited exceptions.[6] Plaintiffs have recently brought chatbot wiretapping claims under Sections 631(a) and 632.7 of the statute, which apply to wire and cellphone communications, respectively.

While California has an exemption for direct party liability, because a party cannot eavesdrop on its own conversation, CIPA provides for liability when a party aids and abets a third party in surreptitious wiretapping.[7]

The California statute also provides for statutory damages of $5,000 per violation, plus treble actual damages and attorney fees.[8] Like Massachusetts, in 2022, California also saw a wave of wiretapping claims against website operators based on session-replay software.

Other states with wiretapping statutes requiring the consent of all parties include Delaware, Florida, Illinois, Maryland, Montana, Nevada, New Hampshire, Pennsylvania and Washington.

As in Massachusetts and California, litigants in Florida and Pennsylvania have started asserting wiretapping claims based on website functions.

Plaintiffs' Efforts to Extend State Wiretapping Laws to Chatbot Functions

In recent years, plaintiffs have targeted tracking cookies and pixels and session-replay technology, which are commonly used on websites to collect data, including keystrokes and mouse movements, and to optimize functionality, accessibility and user experience.

A tracking cookie is a text file set by a website onto a user's browser to collect data concerning that user's browsing activity and can be removed by a user by adjusting browser settings. A tracking pixel is a small and sometimes invisible image with computer code that captures information about a user's browsing activity but does not rely on a browser to function.

Companies using tracking cookies and pixels without users' consent have been held to violate the European Union's General Data Protection Regulation,[9] and the companies using them were early targets of plaintiffs attempting to apply U.S. state wiretapping laws to website data collection.[10]

More recently, plaintiffs have also focused on session-replay activities, where websites use analytics tools to capture website activity data and reconstruct that data into sessions for analysis.[11] These technologies often rely on third-party vendor software that captures website interactions, and records and shares that data with vendors.

Plaintiffs have argued that, when tracking cookies and pixels and session-replay technology

capture communications, these functions run afoul of state wiretapping laws. In Massachusetts and California, plaintiffs in some cases avoided early dismissal and secured significant class settlements.

Chatbot litigation is a product of those early favorable rulings in cookie and pixel tracking and session-replay litigation, applying similar theories to a new website function.

Website chatbots allow users to engage with and receive assistance from AI virtual assistants or human customer service representatives. Chatbot functions are often deployed using third-party vendor software, and when chat conversations are recorded, those vendors may be provided access to live recordings or transcripts.

According to this most recent wave of plaintiffs, recording chat conversations and making them accessible to third-party vendors violates state wiretapping laws, with liability for both the website operator and third-party vendor.

However, there are several reasons why the application of wiretapping laws in this context is inappropriate, including but not limited to legal arguments that:

- For certain jurisdictions, state lawmakers have declined to extend wiretapping laws to these contexts despite multiple rounds of proposed amendments;
- Users who visit websites and use chatbot features have provided implied consent to the collection and use of their data in accordance with the websites' privacy notices;
- Party exceptions — under which the intended recipient of a communication cannot be liable for wiretapping their own conversation — for unauthorized recording will apply when website owners directly use third-party software to process consumer data rather than transmitting it externally;
- In certain circumstances, only data concerning the circumstances of communications, but not the contents of communications, are actually transmitted by wire; and
- Plaintiffs in federal court must demonstrate a concrete injury to have constitutional standing.

Defendants swept up in this newest wave of wiretapping litigation are asserting these legal arguments in early dispositive motion practice with mixed results, and it may be several years before the highest state and federal appellate courts clarify how far plaintiffs may extend wiretapping statutes written decades before the internet was invented.

How Businesses Can Address Growing Chatbot Litigation Risk

Despite these strong defenses, businesses with website chat functions should exercise caution to avoid being in a litigation posture where they need to mount any of these arguments.

While the Federal Trade Commission has cautioned website operators not to mislead customers about the nature of their interactions with AI tools, the agency has yet to issue specific guidance on potential wiretapping concerns.[12]

Similarly, the Consumer Financial Protection Bureau has urged financial institutions to

exercise transparency and caution in using chatbots, but has not yet specifically addressed this topic.[13] However, both agencies have indicated that chatbot functions will be under increased scrutiny in the future.

We expect to see chatbot wiretap claims skyrocket in the coming months, against a backdrop of an already record-breaking year in consumer data privacy class actions.

The threat of this litigation is present in all two-party consent states, but especially Massachusetts and California, and companies should beware that they can be targeted by the same or different plaintiffs and counsel in multiple states.

Companies should not assume that just because they do not offer products or services directly to consumers that they are immune from this threat: Any public-facing website with a chat function is vulnerable to litigation.

In this environment, there is a window of opportunity for businesses to expend on prevention to secure future protection and avoid expensive litigation.

A comprehensive review and update of a company's website for data privacy compliance, including chatbot activities, is advisable. These measures include:

- Incorporating clear disclosure language and robust affirmative consent procedures into the website's chat functions, including specific notification in the function itself that the chatbot is recording and storing communications;

- Expanding website dispute resolution terms, including terms that could reduce the risk of class action and mass arbitration;

- Updating the website's privacy policy to accurately and clearly explain what data, if any, is recorded, stored, and transmitted to service providers through its chat functions, ideally in a dedicated chat section;

- Considering data-minimization measures in connection with website chat functions; and

- Evaluating third-party software vendors' compliance history, including due diligence to ensure a complete understanding of how chatbot data is collected, transmitted, stored and used, and whether the third party's privacy policies are acceptable.

Companies may also want to consider minimizing aspects of their chatbots that have a high annoyance factor — such as blinking notifications — to reduce the likelihood of attracting a suit.

This list is not comprehensive, and businesses should be sure that their legal teams are aware of their website functions and data collection practices.

Bringing a certain amount of skepticism to vendor claims of compliance will serve companies well — it is best to independently verify rather than to rely on vendor representations, particularly as a vendor may have a higher risk tolerance.

Companies should beware that plaintiffs may leverage early court victories in their demands and complaints and may learn from early dismissals to refine their pleading practices.

Conclusion

Consumer data privacy litigation is a fast-evolving area of law with rapidly expanding legal obligations created by active legislatures across the country. In this changing landscape, it is critical to stay on top of the latest developments.

Melanie Conroy and Kathleen Hamann are partners, and Ariel Pardee is an associate, at Pierce Atwood LLP.

The opinions expressed are those of the author(s) and do not necessarily reflect the views of their employer, its clients, or Portfolio Media Inc., or any of its or their respective affiliates. This article is for general information purposes and is not intended to be and should not be taken as legal advice.

[1] Mass. Gen. Laws ch. 214, §1B.

[2] Mass. Gen. Laws ch. 272, §99(C).

[3] Mass. Gen. Laws ch. 272, §99(Q).

[4] Bill H.4347 192nd Legislature (2021-2022), sponsored by Governor Baker. See Bill H.1786, 193rd Legislature (current).

[5] See "Massachusetts seeing wave of 'session replay' suits, Plaintiffs' bar seeks to apply wiretap statute to websites," Massachusetts Lawyers Weekly (July 13, 2023), available at: https://masslawyersweekly.com/2023/07/13/massachusetts-seeing-wave-of-session-replay-suits/.

[6] Cal. Penal Code §§ 630–638.55.

[7] Cal. Penal Code § 631(a).

[8] Cal. Penal Code § 637.2.

[9] A March 2023 decision by the Austrian Data Protection Authority (DSB) held that Facebook tracking pixels directly violated the GDPR, a position shared by other European data protection authorities. The decision is available at: https://noyb.eu/sites/default/files/2023-03/Bescheid%20redacted-EN.pdf.

[10] See e.g., John Doe and Jane Doe, et al. v. Partners Healthcare System, Inc., et al., No. 1984CV01651-BLS1 (Mass. Super. 2021); Doe v. Meta Platforms, Inc. et al., No. 3:22-cv-04293-AGT (N.D. Cal. 2022).

[11] See e.g., Alves v. BJ's Wholesale Club, Inc., No. 22-2509-BLS1 (Mass. Super. 2022); Javier v. Assurance IQ, LLC, No. 21-16351, 2022 WL 1744107 (9th Cir. May 31, 2022).

[12] See Using Artificial Intelligence and Algorithms, Business Guidance/Business Blog, Federal Trade Commission (April 8, 2020), available at: https://www.ftc.gov/business-guidance/blog/2020/04/using-artificial-intelligence-and-algorithms.

[13] See Chatbots in consumer finance, Reports, CFPB (June 6, 2023), available at: https://www.consumerfinance.gov/data-research/research-reports/chatbots-in-consumer-finance/chatbots-in-consumer-finance/.