



“Listen Up” if Your AI Policy Does Not Cover AI Recording Issues – Another Class Action Lawsuit Filed Over Third Party AI Recording Service

By: James Gatto

The use of AI recording tools has become prevalent. Companies’ policies addressing the legal issues with these tools is not yet as prevalent. If your company’s AI policy does not address these issues, it needs to be updated. A [recently filed class action](#) stems from *one* fact scenario where legal issues may arise. It is not the first suit against AI recording and it will not be the last. The lawsuit claims violation of the Federal Wiretap Act, 18 U.S.C. § 2510 *et seq* based on use of a third party service that records and perform AI analysis on calls between a dental company and its patients. Details of this lawsuit are provided below. However, it is important to understand that if your company or your employees use AI recording tools or notetakers, you need to ensure that your AI policy covers all of the necessary issues. These issues can include at least: i) managing and documenting notice and consent; ii) dealing with nonconsenting parties participating in a call being recorded; iii) inaccuracies of AI generated transcripts and summaries; iv) AI generated sentiment analysis/emotion detection; v) confidentiality and privilege issues; vi) retention and/or deletion of recordings; vii) vendor diligence on these tools and approval process for specific tools; and viii) knowing the technical features of some tools that can help mitigate risk and others that can create more risk.

The Lawsuit

The putative class action was filed against Heartland Dental, LLC (“Heartland”)¹ for using a third party AI service provided by co-defendant RingCentral, Inc. (“Ring”) which records and performs AI analysis on calls between Heartland and its patients without notice to the dental patients.² The lawsuit claims this violates the Federal Wiretap Act, 18 U.S.C. § 2510 *et seq.* and particularly, 18 U.S.C. § 2511. It primarily deals with the interception and disclosure of wire, oral, or electronic communications. The activity relates to use of a third party service that recorded patients call with a dental service. The claim is based, in part, on the fact that Ring was not a party to the calls. Yet, Ring listens to and analyzes phones calls in real time using its AI tool.

Allegedly, Heartland incorporated the Ring phone into call center services that it provides to its dental practice partners. As a result, patients calling a local dental practice affiliated with Heartland had their calls listened to and analyzed by Ring and its sophisticated artificial intelligence algorithms. The Plaintiff alleges that patients calling a local dental office are not

¹ Defendant Heartland is a dental support organization (“DSO”) that provides services related to non-clinical aspects of running a practice, such as billing, insurance, staffing, and marketing. Allegedly, Heartland Dental is the largest DSO in the United States and has partnered up with over 1,700 dental practices and over 2,800 doctors nationwide.

² The RingCentral AI is a suite of features that listens to phone calls in the background and analyzes conversations in real-time. The features that make up RingCentralAI include, among others, (i) real-time voice transcription, (ii) call highlights, (iii) automated call summaries and (iv) sentiment voice analysis.

informed that an unknown third-party (Ring) is listening in on the calls and analyzing them using AI without the patients' knowledge and consent. According to Plaintiff, Heartland intercepted or procured another person to intercept sensitive communications between Plaintiff and the Class and their healthcare providers in violation of [18 U.S.C. § 2511](#).

Ring is an entirely separate entity from the local dental clinic, and acts as an unannounced listener and auditor of patients' phone calls. Given the nature of the calls, which include individually identifiable health information about their medical treatments. The Complaint alleges this violates 42 U.S.C. § 1320d-6 of the Health Insurance Portability and Accountability Act ("HIPAA"), which imposes federal criminal liability to anyone who obtains "individually identifiable health information" (or "IIHI") relating to an individual or discloses it to another person.

Additionally, the Complaint alleges that Ring not only listens to and analyzes patient calls on Heartland's behalf, but also uses patient calls for its *own purpose*: to train its AI models and develop its own products and services for other customers. Ring's privacy policy governs the relationship between Heartland and RingCentral. It specifically allows RingCentral to use patient calls to improve its own product. But apparently this is not disclosed by Heartland (or Ring) to Heartland's patients. The Complaint asserts that by agreeing to Ring's terms and implementing Ring's phone systems, Heartland has effectively granted an unknown third-party the ability to eavesdrop on patient phone calls in real-time without patient consent.

Lessons To Be Learned

1. Many companies are using AI recording tools and notetakers.³ In some cases, employees on their own are using these tools, in some cases without company knowledge. Companies need to develop policies on the use of these tools. Failure to do so can lead to lawsuits such as the one addressed above. Yet, this is not the only lawsuit that has been filed against these tools.
2. In addition to the federal wiretapping laws, state laws may be relevant. For example, ([CA Penal Code Section 631\(a\)](#)) imposes civil and criminal liability on individuals that aid and abet third parties who secretly eavesdrop on communications, or intentionally intercept communications without obtaining consent. If you hire a third party service without the appropriate precautions, you may be liable for aiding and abetting.
3. Appropriate notice and consent are necessary. In some states, only one party to a conversation needs to consent. In other states all parties must consent. Notice of recording can be automated with some tools. However, policies need to address how to deal with parties, who are on a call being recorded, but do not provide consent. Various technical options exist in some tools. Other methods for managing non-consenting users can be implemented. But it is important to have a policy that ensures this is addressed.
4. Many recordings will include confidential or privilege information. The policy should address managing these recordings to prevent inadvertent disclosure to intended recipients that may destroy confidentiality and/or privilege. Some tools automatically send the transcript and summaries to all participants. This may not be advisable in some cases.
5. In some cases, recorded calls will cover information that you may not want to keep around as it may be discoverable in a later-filed litigation. In other cases, recordings may need to be maintained for regulatory purposes or for a litigation hold. These and other retention/deletion issues need to be addressed in your policy.
6. AI is notorious for hallucinating, i.e., making up stuff. What if you have an AI generated transcript that is inaccurate and months later the recording is pull up and referenced to determine what was said. This inaccurate transcript could lead to many types of problems. AI policies need to address and prevent this.
7. Some AI recording tools, such as the Ring tool at issue in the litigation are used for AI generated sentiment analysis/emotion detection. Depending on how this information is intended to be used, other laws may be relevant.

³ Many AI recording and note taking tools exist. Some are integrated into other products such as [Zoom AI Companion](#) and [Teams](#). Others are standalone tools such as [Fireflies.ai](#) and [Otter.ai](#). Many others exist.

Emotional AI often processes biometric data (e.g., facial expressions, voice tone, physiological signals), which can be considered sensitive personal data under laws like the EU GDPR and California Consumer Privacy Act (CCPA), among others. Caution needs to be exercised when using these features and your AI recording policy needs to address this.⁴

8. Companies employing third party vendor AI recording or notetaker services need to conduct diligence on the vendor tool and carefully consider the Terms of Service and privacy policy. Where the vendor uses the recording for its own purposes, you should consider whether you want to use that tool. If you do, you need to make sure you check the legal boxes, including providing notice to and receiving consent from your customers. In other cases, you may want to avoid using tools that use the AI recording for their own purposes. For some legal issues, if a third party records for you and only you get the recording, that may simplify some things.

Conclusion

The foregoing are sample issues that can arise with AI recordings and notetakers. Different tools and different use cases can implicate other issues. It is important that each company adopt written policies that are appropriate for their own circumstances. There is no one size fits all policy for these tools. The requirement for thorough diligence on these tools can not be overstated. In addition to this lawsuit, there have been other cases where companies using a third party AI service have faced liability issues for aiding and abetting wire tapping due to the third party's activities. This is an area where legal issues continue to evolve as the features of the AI recording tools evolve. It is important to stay up to date on the technology and legal issues and periodically update your AI policies accordingly. Feel free to reach out if you have questions on these or other AI issues.

⁴ For more information on legal issues with Emotional AI, see [The Price of Emotion: Privacy, Manipulation, and Bias in Emotional AI](#).

For more details, please contact:



James Gatto

Artificial Intelligence Team Co-Leader

[bio](#)

202.747.1945

jgatto@sheppardmullin.com

James Gatto is a partner in the D.C. office of Sheppard Mullin and is Co-Leader of its Artificial Intelligence Team. For over 35 years he has been a thought leader on legal issues with emerging technologies and business models, including over 20 years of experience with AI and open source. He provides strategic advice on all IP, tech transactions and tech regulatory issues. He is an adjunct professor at Ole Miss Law School where he teaches Legal Issues with AI. He has been an invited speaker for the US Copyright Office Listening Session on AI Authorship and the USPTO Listening Session on AI Inventorship Issues. He is an appointed member of the AI/Machine Learning Task Force of the American Bar Association's IP Section. He is also a member of the AI committees of the American Intellectual Property Law Association (AIPLA) and the International Technology Law Association.

This alert is provided for information purposes only and does not constitute legal advice and is not intended to form an attorney client relationship. Please contact your Sheppard Mullin attorney contact for additional information.