Satya's practice focuses on technology transactions, intellectual property, and commercial agreements for startup and growth-stage technology companies across AI, robotics, cloud computing, and emerging tech sectors.

Email: snarayan@gcalaw.com
LinkedIn Newsletter: Techline Brief
Connect on LinkedIn

DOES "THIS MEETING IS BEING RECORDED" ACTUALLY COVER YOUR AI NOTETAKING APP?

Satya S. Narayan
March 5, 2026

Every day, thousands of business meetings are recorded by AI notetaking apps. Most participants click "Join," enter the meeting, and only then see the platform's default recording notice. That casual click may not be enough to make the recording legal — and for businesses operating across multiple U.S. states, the exposure is real. This risk sits at the intersection of rapidly adopted technology and laws written before AI notetaking apps existed.

In some states and circumstances, the virtual conferencing platform's default notice may not be legally sufficient at all. And even where notice is sufficient for the platform's own recording, it may not cover the very different technical architectures and downstream data practices of AI notetaking apps. The core problem is that the platform's default notice may cover only the platform's own recording — not an AI notetaking app initiated by the host or a guest, not the notetaking app vendor, and not the additional capture, processing, retention, or model training activities these tools may perform.

This article covers why the issue matters, how the three main architectures of AI notetaking tools create different legal risk profiles, what recently filed lawsuit**s** signal about emerging legal risk, and what businesses should be doing now. Given how widely these tools are being deployed across organizations of every size, the stakes of getting this wrong**,** particularly in multi-state or high-stakes contexts**,** warrant careful attention.

The Legal Landscape Most People Don't Know About

The federal Electronic Communications Privacy Act (18 U.S.C. § 2511) generally requires only one-party consent to record a private communication. However, federal law expressly permits states to impose more stringent requirements, and a significant number of states including California, Washington, Florida, and Illinois, require every party on a call to consent before it can be recorded where there is a reasonable expectation of privacy. **California** — California's Invasion of Privacy Act (CIPA), codified in Penal Code § 632 among other provisions, is one of the most litigated privacy laws in the country. Recording a "confidential communication" without the consent of all parties is both a crime and a basis for civil liability: up to $5,000 per violation or three times actual damages, plus attorney fees. Class action exposure is real for businesses that record at scale without proper consent.

California courts have signaled that implied consent, where a participant receives clear advance notice that recording will occur and proceeds to join, may be valid, but that notice must come before capture begins. The California Supreme Court confirmed in *Kearney v. Salomon Smith Barney, Inc.,* 39 Cal. 4th 95, 137 P.3d 914 (Cal. 2006), that a business that advises all parties of its intent to record at the outset does not violate CIPA, and that recording without such notice does. The Ninth Circuit reinforced this in *Javier v. Assurance IQ, LLC,* No. 21-16351, 2022 WL 1744107 (9th Cir. May 31, 2022), holding that retroactive consent, obtained only after recording has begun, is insufficient under CIPA. Advance notice is not a formality; it is the minimum required before any recording begins. California is not alone. Washington recognizes advance notice as implied consent (WA Rev Code § 9.73.030). However, Florida's wiretapping statute requires "prior consent" (Fla. Stat. § 934.03) and is widely treated as an all-party consent law with compliance guidance generally requiring explicit consent. Illinois requires consent when a private conversation is recorded surreptitiously (720 ILCS 5/14-2), prompting most compliance guidance to favor explicit consent.

Three Ways Notetaking Apps Work — And Where the Consent Gap May Lie

Not all AI notetaking tools work the same way. There are three primary architectures, and each carries a different legal risk profile.

1. The Notetaking Bot Joins the Meeting as a Participant
Some AI notetaking tools join the call as a visible participant. Unlike a conferencing platform's native recording, they are operated by an external vendor and must be intentionally admitted by a human participant. Under CIPA § 632, the prohibition on recording a confidential communication without all-party consent applies regardless of who is doing the recording — participant, host, or third-party vendor whose bot has been admitted to the meeting.

When a notetaking bot joins, most conferencing platforms display a standard recording notification (for example, Zoom displays “This meeting is being recorded”). What participants may not understand is where the audio is going, whose servers it is being transmitted to, or what will be done with it. Notetaking bots join as participants and access the platform's audio stream, transmitting it in real time to their own external servers, entirely outside the conferencing platform's ecosystem, where it is transcribed, stored, and analyzed. The platform's recording notification discloses that recording is underway but does not disclose to participants that the bot is simultaneously transmitting that audio to its own external servers under entirely separate data practices.

CIPA § 631, the wiretapping provision, adds a separate layer by prohibiting unauthorized third-party interception of communications. It contains a "participant exception," meaning a party to the communication cannot wiretap its own conversation. Whether a notetaking bot vendor can claim that exception, on the grounds that it acts as an agent of the host, or whether it is instead an unauthorized third-party interceptor, is an open question before the courts.

In *Graham v. Noom, Inc.*, 533 F. Supp. 3d 823 (N.D. Cal. 2021), the court held that a session replay vendor that captured data and hosted it on its own servers solely on behalf of the website operator was not a third-party eavesdropper. By contrast, in Yoon v. Lululemon USA, Inc., 549 F.Supp.3d 1073 (C.D. Cal. 2021), the court indicated that whether the 'participant exception' applies turns on what the vendor actually does with the data, not merely on the fact that a first-party user enabled the tool, and reserved that question for the jury. If the vendor processes and retains data solely on behalf of the host, *Graham* may apply. If the vendor uses that data for its own model training or product development, *Yoon* is more likely to govern, and the “participant exception” may not be available as a defense. **These risks are no longer theoretical: *In re Otter.ai Privacy Litigation*.** Filed beginning in August 2025 and consolidated in October 2025 in the Northern District of California (No. 5:25-cv-06911), this putative class action consolidates multiple complaints, including *Brewer v. Otter.ai* and *Walker v. Otter.ai,* and has been assigned to Judge Eumi K. Lee. The cases remain in the early case management phase as of early 2026.

The *Brewer* complaint alleges that Otter’s Notetaker and OtterPilot tools automatically join Zoom, Google Meet, and Microsoft Teams meetings and record, access, and transmit the contents of conversations in real time, including conversations of participants who are not Otter account holders and who allegedly received no meaningful disclosure that a third-party AI vendor would be capturing their statements. The named plaintiff, a non-account holder, asserts that he participated in a Zoom meeting in February 2025 without any reason to know his conversation would be retained and used for machine learning purposes by Otter.

The *Walker* complaint adds allegations that Otter captures “voiceprints,” which plaintiffs characterize as unique biometric identifiers, thereby implicating state biometric privacy laws such as Illinois’ BIPA. Across the consolidated litigation, the complaints assert claims

under CIPA, ECPA, the CFAA, California's CDAFA, California's Unfair Competition Law, and common law causes of action including intrusion upon seclusion and conversion.

Central to the plaintiffs' theory is a passage in Otter's own privacy policy acknowledging that it trains its AI on de-identified audio recordings and on transcriptions that may contain personal information. Plaintiffs contend these practices constitute the use of meeting content for the vendor's own model development which, under their ECPA theory, they allege defeat the one-party consent exception by constituting an independent tortious purpose. Otter disputes the complaints' characterization of its data practices. No findings of fact or law have been made, and the litigation remains at the early case management stage. The case nonetheless illustrates precisely the consent and downstream use questions that arise when AI notetaking tools access and process meeting content at scale.

Risk summary: The conferencing platform typically faces limited exposure as platforms generally disclaim responsibility for recording compliance and third-party integrations by contractually shifting such responsibility to the meeting host through their terms of service to which the host has agreed. The notetaking bot vendor potentially faces exposure under § 632, and possibly, § 631. The host bears the most direct exposure — they admitted the bot and have the primary obligation to ensure all participants meaningfully consented.

2. The Platform-Integrated Notetaking App: The Platform Records, the App Receives

Some AI notetaking applications do not join the meeting at all. Instead, they integrate directly with the conferencing platform and receive a copy of the platform's own native recording after the meeting concludes. Once the integration is enabled, the platform records the meeting using its built-in function, triggering its standard recording notification to participants. After the meeting ends, the notetaking app automatically retrieves that recording via API, processes it, and stores the output. The notetaking app typically does not appear in the meeting.

At first glance, this model appears cleaner from a consent standpoint. But the consent analysis does not end there. The *Graham/Yoon* framework turns on what the vendor does with the content once it receives it. That question is no less relevant here than in the bot context, and may be more consequential. Where a notetaking bot joins a meeting, at least a visible participant appears in the meeting list. In the platform-integrated model, the notetaking app vendor may be entirely invisible. Participants may have no signal, before, during, or after the meeting, that their conversation will be transmitted to and processed by a third party.

Platform consent and application-specific consent are also legally distinct. A participant who saw the platform's standard recording notification was told that the platform was recording, nothing more. That notification says nothing about an off-platform third-party vendor subsequently receiving and processing the meeting content. Indeed, platforms

themselves typically disclaim any responsibility for third-party integrations built on top of their services. For instance, Zoom's Terms of Service makes this explicit: it states that use of any third-party offering is "governed solely by the terms of such Third-Party Offerings," and its Privacy Statement separately provides that personal information shared with third-party apps is "collected and processed in accordance with the app developers' terms and privacy policies, not Zoom's."

Risk summary: The conferencing platform faces limited exposure where it has provided adequate notice for its own recording. The notetaking app vendor's exposure turns on the *Graham/Yoon* distinction. The host, having enabled the integration, bears responsibility for ensuring participants were informed not just that recording was occurring, but that a specific notetaking app would receive and process the content under entirely separate data practices. Risk to the host is moderate for the platform recording itself but might be elevated with respect to the further downstream AI processing that the host did not inform the participants about.

3. The Local Audio Capture App

Some tools, including browser extensions, desktop applications, and mobile apps, capture audio directly from a user's device through the microphone, system audio output, or a browser-level hook. The capture happens silently, on one participant's device, invisible to everyone else. Bluedot records in the background across major conferencing platforms without appearing as a meeting participant. Tactiq works as a Chrome extension that captures live captions directly in the browser, with no bot, no platform recording trigger, and no separate participant entry.

This is the most legally precarious architecture of the three. Because the notetaking tool captures audio directly on a participant's device rather than through the platform, no conferencing platform recording notification is generated, and under Kearney and Javier, that gap cannot be cured after capture has begun. Some notetaking tools in this category offer optional notification mechanisms, such as an in-meeting chat message, that the host can use to inform participants that recording is underway. In some cases these notifications are not enabled by default. None are mandatory, and the decision whether to use them rests entirely with the host.

Risk summary: The conferencing platform faces no exposure. The local capture vendor's direct exposure is more limited, as the host bears the primary obligation to obtain consent. The entire burden of obtaining advance, informed consent from every participant falls on the host. In all-party consent states, this is the highest-risk architecture of the three.

The Consent Gap Nobody Is Talking About

The common thread across all three models is the distance between the platform-level recording notice and application-specific consent for the notetaking app. When a

conferencing platform tells you a meeting is being recorded, participants understand that the platform is recording. Most do not understand, because they are not told, that a third-party AI application is simultaneously receiving or accessing that recording, transcribing it, summarizing it, and in some cases using it to train models.

That gap is where the legal exposure lives. The conferencing platform's recording notification was designed for the platform's recording. It was not designed to disclose a parallel ecosystem of third-party tools that may be operating during the same call, processing the same audio, and operating under entirely different data practices that participants may never have been told about and whose terms they may never have agreed to.

What makes this particularly difficult from a compliance standpoint is that many employees using these tools have no idea there is a problem. AI notetaking apps are marketed as productivity tools, not as legally complex data collection systems. The default assumption, that the meeting platform's built-in recording notice covers *everything*, is widespread and understandable. It is also, in many circumstances, legally unsupported. In most organizations, employees are already using these tools without any formal guidance, and the compliance exposure that it creates belongs to the company, not just the individual host.

Categories That Deserve Extra Attention

Some meeting types carry heightened risk where advance notice alone may be insufficient:

• **Multi-state meetings** — as a compliance practice, if any participant is located in a stricter all-party consent state (e.g., California or Florida), businesses should typically default to the most restrictive consent standard applicable to that participant's jurisdiction.
• **International meetings** — GDPR and analogous frameworks treat voice recordings as personal data with independent consent requirements that U.S.-centric notetaking app defaults may not satisfy.
• **Meetings involving third-party confidential information** — consent to record does not substitute for authorization to disclose. Routing meeting content through a notetaking app that uses any content to improve its own services may independently trigger confidentiality obligations under an NDA or trade secret framework.
• **Meetings involving legal counsel** — routing privileged communications to a third-party notetaking app may waive attorney-client privilege, particularly where the vendor uses that content for its own purposes. That risk exists regardless of whether recording consent was properly obtained.
• **Regulated industries** — in financial services, healthcare, and similar fields, the standard AI notetaking app's default recording notice is not designed to navigate the additional recording and data obligations these contexts impose.

• **Employment negotiations**— notice alone is often insufficient in all-party consent states; explicit, documented consent is the safer standard.
• **Government meetings -** for meetings with government and regulatory bodies, agency-specific rules and regulatory requirements may independently govern how communications are handled and retained.

What Businesses Should Actually Do

- **Stop relying on platform notices alone.** A conferencing platform's recording banner was designed for the platform's own recording function. It may not adequately cover an AI notetaking app that will receive and process the same content under entirely separate data practices. Treating the conferencing platform notice as a complete solution is the single most common compliance mistake organizations make in this space.
- **Use the tools your platform and notetaking app already provide.** Most conferencing platforms and many notetaking app vendors offer optional pre-meeting notices, in-meeting alerts, consent prompts, or administrative settings that allow hosts to disclose third-party recording and obtain confirmation in advance. These features exist precisely because the default notice is often insufficient. Businesses should review and enable them where appropriate, rather than leaving them off because they require an extra step.
- **Use explicit, app-specific consent.** Before any meeting where an AI notetaking app will be used, participants should know which application is in use, what it does with their data, and where to find its terms and privacy policy. A general statement that the meeting "may be recorded" is not enough. In high-stakes contexts, get the participants' acknowledgement through an affirmative confirmation mechanism before the meeting begins.
- **Have a clear internal policy.** Specify which tools are approved for recording and notetaking, when they may be used, what consent must be obtained before use, and how recordings and transcripts are handled and retained. Without a written policy, individual employees will make their own judgments, and those judgments will not always be legally sound.
- **Audit your current stack.** Know which applications your teams are using, how they work technically, and whether your current consent practices match the legal requirements of the states where your participants are located. Many organizations discover, when they look carefully, that multiple notetaking tools are in active use across different teams, with no consistent policy governing any of them.

The Bottom Line

AI notetaking tools are genuinely useful, and the efficiency gains they offer are real. Businesses need to acknowledge that adoption is not going to reverse. But the platform's default recording notice tells participants only that the platform is recording. It does not tell them that an AI vendor may be separately accessing, transmitting, analyzing, storing, or

training models on the meeting content. The legal frameworks these tools operate within have not caught up with the technology, and the gap between what conferencing platform notices cover and what notetaking apps actually do is a compliance problem businesses need to address proactively — not reactively, after a complaint has been filed.

The *In re Otter.ai* litigation is an early indicator of where plaintiffs' lawyers are looking. It will not be the last case in this space. As these tools become more deeply embedded in how organizations operate, the absence of a clear consent framework and internal policy will become increasingly difficult to defend.

The companies that get ahead of this will have clear policies, explicit consent practices, audited tool stacks, and employees who understand what they are permitted to use and when. The ones that don't will eventually find out the hard way that "this meeting is being recorded" does not cover everything they thought it did.
