AI Meeting Tools Are The Latest Target of Illinois BIPA Class Actions – 6 Things to Do to Prevent Litigation

Insights
1.23.26

The latest BIPA target serves as both a reminder and a warning shot that AI notetaker apps and other listening tools could run afoul of the state's strict privacy law. A recent proposed class action filed on December 18 alleges a popular AI notetaker vendor violated the Illinois Biometric Information Privacy Act (BIPA) when it allegedly collected and stored voiceprints during a virtual meeting without proper notice, consent, or a compliant data retention policy. While the case targets the AI vendor, the allegations carry important lessons for Illinois employers and any multistate employer with Illinois employees in the room during a virtual meeting. Here's a recap of what's going on and six practical steps you can take to minimize your chances of facing legal liability.

What Happened: Familiar Workplace Scenario Turns Into Lawsuit

The facts alleged in the complaint may sound uncomfortably familiar to many employers.

- An Illinois resident joined a routine virtual meeting.
- She never signed up for any AI meeting assistant.
- She never clicked "I agree" to any terms of service.
- But an AI notetaking tool automatically joined the meeting at the request of one of the participants.
- Like AI notetaker tools are supposed to do, it recorded the discussion, identified speakers, and generated transcripts attributing statements to individual participants (among other things).

According to the December 18 lawsuit filed by Katelin Cruz in an Illinois federal court, that process required the notetaker to create and store "voiceprints," which may be considered "biometric identifiers" under BIPA. And BIPA requires businesses that collect voiceprints and other biometric identifiers to jump through certain hoops *in writing* before a biometric information is collected.

Cruz's lawsuit alleges that the AI vendor violated BIPA because it didn't jump through several of those key hoops. Specifically, it never informed her in writing that it was collecting her biometric data, never informed her in writing how long it would be retained, and never gave her the option of providing written consent. She further claims the ai notetaker vendor failed to publish a compliant biometric data retention and destruction policy, also required by BIPA.

As always, the claims in Cruz's lawsuit remain allegations, and the AI vendor has not yet even started to defend the lawsuit and tell its side of the story. But in Illinois and across the country, allegations alone can often be enough to trigger expensive litigation.

Why This Matters for Illinois Employers (and Those With Illinois Employees)

At first glance, employers might see this lawsuit as an immediate issue. After all, the AI vendor is the target of this lawsuit, not the meeting host or employer. But that's a risky assumption. Indeed, lawsuits against the technology vendors often are the precursor to lawsuits against the technology customers.

Illinois's BIPA is unusually strict and enforced almost entirely through private lawsuits. Courts have made clear that more than one entity can be liable for the same biometric collection or disclosure, depending on who enabled the technology, benefited from it, or failed to control its use.

Employers can get pulled into BIPA litigation in several common ways, including:

- **Authorizing or deploying the tool** – If your organization selects, licenses, or encourages use of an AI notetaker that captures voiceprints without proper notice and consent, plaintiffs may argue you participated in the biometric collection.
- **Employee use during work-related meetings** – Even when an individual employee activates an AI assistant, plaintiffs may attempt to tie that conduct to the employer if it occurs during meetings held for business purposes.
- **Benefiting from the outputs** – Transcripts, searchable archives, or performance insights generated from AI tools can support claims that the employer received an derived value from biometric data.
- **Lack of guardrails** – Illinois courts have shown little patience for arguments that biometric collection was "automatic" or "incidental." Missing policies, approvals, or training can become part of the liability narrative.

Location also matters. An employer headquartered outside Illinois can still face BIPA claims if meetings include participants physically located in Illinois, even if the vendor is based elsewhere.

This lawsuit also fits into a broader trend. As AI tools increasingly rely on voice and other potential or alleged biometric data, plaintiffs' lawyers are testing how those tools intersect with BIPA. And courts have made it clear that process matters when biometric data is involved. Those deploying this technology need to evaluate written notice, consent, retention limits, and transparency up front (which can prevent you from being served with a lawsuit).

6 Steps Employers Should Take Now

Employers don't need to abandon AI notetaking, but you do need to govern it effectively given this lawsuit and the impending flood of claims we may see in the coming months and years. With that in mind, this is a good moment for employers operating in Illinois (or with an Illinois presence) to tighten their approach to AI meeting tools. Here are six practical steps to consider:

1. Inventory AI Meeting Tools in Use

Identify which platforms, plug-ins, and "auto-join" assistants your employees are using across your entire organization. Make sure you don't just consider those official tools approved by your organization but that your sweep includes the tools deployed by individual employees or departments.

2. Understand What the Tool Actually Collects

Don't rely on marketing labels that describe the tool as simply being a "transcriber" or "notetaker." Determine whether the tool performs speaker recognition, voice identification, or other functions that could involve biometric data. Tools that identify speakers, distinguish voices, or tie transcripts to individuals are operating squarely in biometric territory and implicate BIPA.

3. Clarify Who Can Enable Recording or AI Assistants

Consider restricting who may activate AI notetakers in meetings, especially those involving external participants (that could include Illinois employees). Regardless of where you or your AI vendor are located, BIPA can still apply if your virtual meetings involve participants physically located in Illinois.

4. Update (and Enforce) Meeting and Recording Policies

General privacy policies or passive participation in a meeting may not be enough to satisfy BIPA's strict terms. Make sure your policies clearly address when AI tools may be used, how participants are to be notified, and what approvals you'll require before deployment.

5. Coordinate With Vendors, But Don't Outsource Compliance

Vendor assurances help, but they do not replace your own risk assessment. Courts are likely to not accept a finger-pointing defense if you haven't conducted sufficient due diligence with your AI vendors. Confirm whether they have BIPA-specific consent mechanisms and retention policies, and document those discussions so you have a ready defense should problems arise.

6. Train Employees on "Meeting Hygiene"

Employees should understand that enabling an AI assistant is not a neutral act. A short training or guidance memo can go a long way in reducing accidental exposure.

Conclusion

Our FP Privacy and Cyber Group attorneys, hand-in-hand with our AI attorneys, will continue to monitor the status of this and other BIPA litigation, so make sure you are subscribed to Fisher Phillips' Insight System to receive the most up-to-date information directly in your inbox. If you have questions about how this lawsuit may impact your business practices, reach out to the author of this article, your Fisher Phillips attorney, or any attorney in our Chicago office.

Related People

Danielle Kays
Partner
312.260.4751
Email

Service Focus

Privacy and Cyber

Consumer Privacy Team

AI, Data, and Analytics

Litigation and Trials

Related Offices

Chicago