From Timeclocks to AI Notetakers: Biometric Privacy in the Age of Artificial Intelligence

A single social media feature alleged to have scanned facial geometry without consent generated a $650 million settlement. A facial recognition database that scraped from publicly available photos led to $52 million+ in multistate settlements and regulatory action. Now, a new wave of lawsuits is targeting artificial intelligence ("AI") technologies used in connection with video conferencing, resume/candidate screening, call-center systems, drive-thrus, and workplace monitoring software—standard features of how organizations operate today. Organizations that never thought of themselves as "biometric collectors" may now be exposed to potentially significant legal risk.

The key accusation in many of these suits is not that a company scanned a fingerprint or retina, but that AI software analyzed ordinary audio or video and generated "biometric information" behind the scenes. Biometric litigation is no longer just about timeclocks and fingerprints. Any organization deploying AI tools that may analyze faces, voices, or other uniquely human characteristics, whether for meetings, analytics, security, or productivity should revisit its biometric risk assumptions.

This alert explores how and why BIPA lawsuits are increasingly targeting AI-enabled tools, what t rends are emerging in those cases, and what developments organizations should be monitoring going forward.

A Brief Reminder: What Biometric Privacy Statutes Regulate

The Illinois Biometric Information Privacy Act ("BIPA") has been one of the most active and aggressively litigated privacy statutes in the United States for years. But biometric privacy is not an Illinois-only concern. An organization operating in multiple states must manage a patchwork of notice standards, consent mechanisms, retention timelines, prohibitions, and enforcement schemes. There is also a full pipeline of pending biometric and AI legislation. See: U.S. biometric laws & pending legislation tracker; US state-by-state AI legislation snapshot.

The Illinois BIPA regulates the collection, use, storage, and disclosure of certain forms of "biometric identifiers" (retina or iris scans, fingerprints, scans of hand or face geometry, and voiceprints) and "biometric information" ("any information, regardless of how it is captured, converted, stored, or shared, based on an individual's biometric identifier used to identify an individual"). The statute has been powerful because it:

- Requires written notice and consent
- Mandates a biometric retention and destruction policy
- Includes a private right of action with liquidated statutory damages
- Has been held to not require proof of actual damages

For years, this combination has made BIPA a favorite of class action plaintiffs and counsel.

The First Wave: Hardware Based Biometrics

When BIPA litigation surged after the Illinois Supreme Court's 2019 Rosenbach decision, most cases fell into a familiar pattern:

- Fingerprint and hand-based timekeeping systems
- Access control devices
- "Try on" technologies
- Employer-employee disputes arising from workplace practices

These cases are mostly focused on tangible devices. Compliance failures were often procedural—no written consent, no posted policy, or improper data sharing.

That landscape, however, no longer reflects the full scope of biometric privacy risk.

The New Center of Gravity: AI-Driven Software

Plaintiffs are now training their sights on software based AI systems rather than physical scanners. These legal theories are contested, and in many instances have not been definitively resolved by courts. Nevertheless, they represent areas of active litigation risk that organizations should assess proactively.

Common targets now include:

Voice analytics — conferencing platforms, AI assistants and transcription software, and call centers

Facial recognition — surveillance, performance feedback, and video interview analysis

Emotion, engagement, or sentiment analysis — tools that infer emotional states or attentiveness from facial expressions, vocal tone, or other behavioral cues

AI hiring and HR tools — automated video interview scoring, resume screening, and employee productivity monitoring

Why AI Tools May Be Particularly Vulnerable To Litigation

Three characteristics of modern AI systems make them especially attractive targets for BIPA claims.

1 Fact-Intensive Nature of Allegations that AI "Derives" Biometrics from Ordinary Data

Plaintiffs argue that AI systems violate BIPA even when they do not store raw data. Instead, they allege that the following qualify as "biometric information":

- Facial geometry extracted from video
- Voiceprints generated from speech
- The mathematical representations that AI models create from faces or voices — commonly called "templates" or "embeddings"

Defendants frequently argue that AI systems:

- Do not collect or store biometric identifiers or information
- Rely on anonymized or transient processing
- Are not actually used to identify an individual
- Use probabilistic models rather than identification

While these arguments may ultimately prevail, courts have, at times, treated these allegations as fact-intensive, particularly where AI models and data flows are opaque to those not intimately familiar with the technologies. The result is increased defense cost, leverage for plaintiffs, and pressure to settle early.

2 AI Expands the Universe of Defendants

Another notable shift is who gets sued. Traditionally, BIPA cases targeted employers. Now, plaintiffs name:

- AI software vendors and SaaS providers
- Platform operators and technology intermediaries
- Consumer-facing companies that deploy AI tools

3 Scale Still Matters—Even After the Damages Cap

In 2024, Illinois amended the BIPA to limit damages to one recovery per person per method, responding to concerns about "annihilative liability." In 2026, the Seventh Circuit Court of Appeals confirmed that this amendment applies retroactively.

That development unquestionably reduces theoretical exposure. But it has not eliminated incentives to sue. Plaintiffs now emphasize:

- Large putative class sizes
- Allegations of willful or reckless conduct
- Novel AI uses that test the boundaries of the statute

AI tools, by their nature, are scalable. Even capped, damages can still be significant when applied across a large number of individuals.

Where Biometric Litigation is Headed Next

Looking ahead, several trends are likely to accelerate:

- Continued lawsuits targeting voice-based AI and multimodal AI systems
- More disputes over whether AI inference equals biometric "collection"
- Increasing overlap between BIPA, AI governance, and consumer protection theories

Even in the wake of legislative reform, BIPA remains a potent instrument for plaintiffs—and biometric litigation has evolved well beyond its origins in timeclocks and fingerprint scanners. AI has fundamentally reshaped the biometric risk landscape, drawing in organizations that may never have considered themselves biometric data collectors.

As AI adoption accelerates and AI-powered features proliferate across enterprise software, organizations must remain vigilant. Many platforms are embedding capabilities—such as voice analytics, facial recognition, and sentiment analysis—that may collect or derive biometric data by default, often without the knowledge of legal or compliance teams.

Organizations should work with legal counsel to audit their technology stack, assess whether AI-enabled features may trigger biometric privacy obligations, and ensure that new tools and updates are reviewed before deployment. Those that take a proactive approach to AI and biometric risk assessment will be better-positioned to defend against these claims and demonstrate good-faith compliance efforts.