Stay Current

PAUL HASTINGS

April 2026

Follow us on LinkedIn

Litigation Update

Double Trouble: Where Biometrics and AI Converge, Exposure Compounds

By Aaron Charfoos, Michelle A. Reed and Sarah E. Hintzen

Companies are increasingly combining biometric information with artificial intelligence (AI) tools — and privacy plaintiffs are taking notice. The collection of biometric information and use of AI each independently present their own legal risks. When they are used together, these exposures compound. Companies should act early to address each regulatory framework simultaneously and take the steps outlined below to mitigate risk.

The New Wave of Biometric Litigation Targets AI

A new wave of biometrics litigation has arrived. Initially, much of the biometric litigation was around the use of fingerprint-based time clocks by employers. When these types of cases subsided, the next iteration of biometrics class actions focused on facial scanning of consumers — especially use cases like virtual makeup try-on technology. Once more, the landscape is shifting, and this time plaintiffs are capitalizing on AI.

Two recently filed class actions alleging violations of Illinois' Biometric Information Privacy Act (BIPA) against two AI notetaking apps, Fireflies.ai and Otter.ai, are good examples. The complaints allege that these transcription tools analyze speakers' voices and generate voiceprints to attribute statements to individual participants without proper notice and consent.

Even more recently, a class action complaint was filed against two healthcare providers in California under statutory and common law privacy theories based upon their use of an AI tool to record and transcribe physician-patient conversations without providing clear notice and obtaining consent. Although the complaint does not focus on biometric information, it serves as a reminder that companies using AI transcription tools — not just the companies developing them — and companies outside of states where biometric information is strictly regulated, are not immune from the risks they carry.

These cases are too new to know how the courts will rule on these issues. However, they are a preview of what is to come as AI transcription and summarization applications have exploded in popularity. Although potentially very useful, these tools may come with unexpected legal consequences. In this instance, not only is there a risk of biometrics litigation with AI notetaking tools but also a host of other legal concerns, including the accuracy and discoverability of the transcripts produced, potential capturing of sensitive or privileged conversations, and the implication of eavesdropping statutes, especially in states requiring consent from all participants to a recorded conversation.

Although the risk of processing biometrics is heightened in Illinois where BIPA's private right of action drives class actions, the scope of exposure is not limited to one state, as shown by a proposed class action filed against Photobucket in Colorado federal court.[1] This case alleges that Photobucket, an image-hosting website, unlawfully threatened to sell billions of photos uploaded by users so that their biometric data can be used to train AI. The plaintiffs have raised theories under a wide variety of privacy and consumer protection laws, including BIPA, as well as theories grounded in contract and common law.

As plaintiffs' firms actively recruit clients for class actions involving the input of biometrics into AI models, the threat of similar actions will only grow. To get ahead of this trend, companies should consider how their processing of biometric information and use of AI may be targeted under various statutes and theories in different states.

New Regulations Spell Trouble for Predictive Analytics Using Biometrics

Predictive analytics, especially when used to aid in decision-making, is one area in particular that could yield substantial litigation in the near future. New laws and regulations have arisen specifically targeting automated decision-making technology (ADMT). Predictive analytics use historical data to predict the likelihood of future outcomes. ADMT leverages these predictions to assist or replace discretionary decision-making by humans.

The latest in a series of laws directly regulating ADMT is Colorado's AI Act (SB 24-205), which is now scheduled to take effect on June 30, 2026. Colorado Gov. Jared Polis moved the effective date back from February 1, 2026, when lawmakers were unable to reach a compromise on amendments to the original law. The Colorado AI Act regulates the development and use of "high-risk" AI systems that make consequential decisions materially affecting the provision or denial, or the cost or terms of education enrollment or education opportunities, employment or employment opportunities, financial or lending services, essential government services, housing, insurance and legal services.[2] The law requires companies, among other things, to implement risk-management and monitoring practices, provide certain disclosures (such as informing users when they interact with AI) and document efforts to reduce bias.[3]

The extent of human involvement is a significant factor in determining liability. The Colorado AI Act excludes systems that detect decision-making patterns and are not intended to replace previously completed human assessments.[4] Similarly, the California Consumer Privacy Act's (CCPA's) regulations concerning ADMT apply only when a business uses the technology's output to make a decision without "human involvement," as defined therein. These ADMT provisions went into effect alongside other CCPA regulations at the beginning of 2025, as we covered previously. As such, the risks of ADMT can be mitigated by having greater human oversight of any decisions it may recommend.

As discussed, there is an inherent risk to technology that combines biometrics with AI. When ADMT, specifically, relies on biometric information as an input, legal exposure is further heightened given the dedicated regulatory frameworks for ADMT. For example, HireVue, which offers an automated video-interview platform that uses face and voice biometrics to evaluate traits such as personality and cognitive ability in job applicants, has contended with actions under both BIPA and anti-discrimination laws.

Moreover, there have been creative theories upon which plaintiffs have targeted HireVue. A Massachusetts resident filed a complaint against HireVue after learning that the company analyzed his interview through Affectiva technology to track facial expressions such as "smiles, surprise, contempt, disgust, and smirks," which then assigned candidates an "employability score."[5] The plaintiff relied on a novel theory that the assessment was a "lie detector" test, arguing that under Massachusetts law, it is unlawful to require or administer a lie detector test as a condition of employment. The plaintiff highlighted that part of the employability score included analysis of a candidate's "conscientiousness and responsibility," including a candidate's "innate sense of integrity and honor."

This case serves as a reminder that plaintiffs can find unconventional ways to challenge new technologies. The use of predictive analytics to evaluate job applicants is a prime example of how the intersection of biometrics and AI can be especially problematic. Illinois even has a separate act directly addressing AI hiring, titled the Artificial Intelligence Video Interview Act, prohibiting employers from using AI to evaluate applicants without first obtaining consent.

It would not be surprising to see additional types of ADMT technologies targeted as they become more commonplace. The existing rise of cases involving biometric information and AI, in conjunction with a regulatory focus on predictive analytics, means companies should exercise caution when using ADMT, particularly in making hiring and performance decisions.

How to Mitigate Risk

To mitigate risk, companies deploying AI systems that rely on biometric inputs should take the following measures:

- **Implement clear notice and consent mechanisms** for collection of biometric information that comply with all applicable laws, especially BIPA. These mechanisms should be in place when biometric data sets are purchased or biometric information is collected by third-party vendors on behalf of the company.
- **Conduct AI impact or risk assessments** prior to deployment, consistent with requirements under the Colorado AI Act, the CCPA's ADMT regulations and other emerging frameworks.
- **Ensure a human is involved in all decision-making**, even when AI provides recommendations. Human oversight is a key mitigating factor under both the Colorado AI Act and the CCPA's ADMT regulations.
- **Document all efforts** to comply with biometric and AI governance regulations.
- **Audit third-party AI tools** — including transcription, notetaking and video-interviewing platforms — for biometric data processing that may occur without the company's knowledge or express consent.

✧ ✧ ✧

If you have any questions concerning these developing issues, please do not hesitate to contact any of the following Paul Hastings lawyers:

Chicago

Aaron Charfoos
+1-312-499-6016
aaroncharfoos@paulhastings.com

Sarah Hintzen
+1-312-499-6096
sarahhintzen@paulhastings.com

Dallas

Michelle Reed
+1-972-936-7475
michellereed@paulhastings.com

[1] *Pierce et al. v. Photobucket, Inc.*, D. Colo., 1:24-cv-03432, complaint filed 12/11/2024.

[2] C.R.S. § 6-1-1701(3).

[3] C.R.S. §§ 6-1-1702, 6-1-1703, 6-1-1704.

[4] C.R.S. § 6-1-1701(9)(b)(B).

[5] *Baker v. CVS Health Corporation et al.*, D. Mass., 1:23-cv-11483, complaint filed 04/28/2023.