

OCTOBER 29, 2026 | PUBLICATION

Client Alert: When AI-Generated Images Trigger Biometric Privacy Risks: New Lawsuits Highlight Emerging Compliance Challenges for Businesses

INDUSTRY SECTOR

Technology

SERVICE LINE

Data Privacy
Technology

RELATED PROFESSIONALS

C. Jade Davis

MEDIA CONTACT

Wendy M. Byrne
wbyrne@shumaker.com

Generative artificial intelligence (AI) applications that transform photographs into professional headshots, avatars, and other digital images are facing heightened scrutiny under Illinois' Biometric Information Privacy Act.

AI is transforming how businesses create, edit, and use digital images. From AI-generated professional headshots and virtual try-on tools to personalized avatars and marketing content, companies increasingly rely on applications that process photographs of employees, customers, and consumers.

But as these technologies become more commonplace, a new wave of privacy litigation is raising an important question: When does an ordinary photograph become regulated biometric information?

Recent class action lawsuits involving Grok, the generative AI platform developed by xAI, illustrate how longstanding biometric privacy laws may create new legal exposure for businesses deploying AI-powered image technologies.

The litigation also serves as a reminder that businesses do not necessarily need to use traditional facial recognition or identity verification systems to encounter biometric privacy risks. Depending on how an AI application processes facial features, even seemingly routine image-generation functionality may warrant closer scrutiny.

New Litigation Targets AI-Generated Images

In October 2026, plaintiffs filed putative class action lawsuits in the U.S. District Court for the Northern District of Illinois alleging violations of the Illinois Biometric Information Privacy Act (BIPA) arising from

Grok's processing of user-uploaded photographs.

The complaints reportedly involve consumers who uploaded personal photographs and requested AI-generated images, including professional headshots and stylized portraits.

According to the allegations, the platform analyzed or extracted facial geometry from those photographs to generate the requested images without providing the disclosures, obtaining the written releases, or maintaining the publicly available retention and destruction policies required by BIPA.

The plaintiffs contend that the alleged processing constitutes the collection of biometric identifiers or biometric information, even though the original photographs themselves fall within a statutory exclusion.

The lawsuits remain in their early stages. The allegations have not been established, and whether the underlying technology actually performs biometric processing within the meaning of BIPA remains a central legal and technical question.

Nevertheless, the litigation highlights an emerging area of risk for organizations developing, licensing, or incorporating generative AI applications into their operations.

Why the Distinction Between Photographs and Facial Geometry Matters

BIPA, enacted in 2008, imposes specific obligations on private entities that collect, capture, purchase, receive through trade, or otherwise obtain biometric identifiers or biometric information.

The statute identifies a "scan of hand or face geometry" as a biometric identifier but expressly excludes photographs from that definition. This distinction is significant.

A business may reasonably understand that collecting a customer's photograph does not, by itself, constitute collecting a biometric identifier under BIPA. However, the legal analysis may change when software processes that photograph to extract facial measurements or other information that qualifies as biometric data.

For example, an AI-powered application might analyze facial landmarks, relative distances between facial features, or other characteristics to generate a realistic digital likeness.

Whether such processing constitutes a regulated scan of face geometry depends on the technology's actual operation and the applicable legal interpretation.

Importantly, not every application that edits or transforms a photograph necessarily collects biometric identifiers. The mere use of AI to process an image does not automatically establish a BIPA violation.

The emerging litigation instead focuses attention on what happens to the photograph after it is uploaded, including what information is derived from the image, how that information is used, and whether it is retained or disclosed.

For businesses, that distinction makes understanding the underlying technology particularly important.

BIPA Creates Significant Compliance Obligations and Litigation Exposure

Unlike many state privacy laws, BIPA provides a private right of action, allowing individuals to pursue claims directly against businesses for alleged statutory violations.

Under Section 15(b), covered private entities generally must satisfy several requirements before collecting or otherwise obtaining biometric identifiers or biometric information, including:

- Providing written notice that biometric information is being collected or stored;
- Informing individuals in writing of the specific purpose and length of time for which the information will be collected, stored, and used; and
- Obtaining a written release from the individual or the individual's legally authorized representative.

Section 15(a) separately requires covered entities possessing biometric identifiers or biometric information to develop a written policy, made available to the public, establishing retention schedules and guidelines for permanently destroying the information.

BIPA also regulates the disclosure, sale, storage, and protection of covered biometric data.

The potential financial consequences can be substantial. The statute authorizes liquidated damages of \$1,000 for each negligent violation and \$5,000 for each intentional or reckless violation, or actual damages if greater, along with other available relief.

Although Illinois amended BIPA in 2024 to limit repeated recoveries involving the same person's biometric data under certain provisions, the statute continues to present meaningful class action exposure.

For businesses operating consumer-facing applications at scale, even allegations involving a relatively small percentage of users can create significant litigation and defense costs.

The Risk Extends Beyond AI Developers

One of the most important lessons from the Grok litigation is that biometric privacy exposure may not be confined to companies developing foundational AI models.

Businesses increasingly integrate third-party AI capabilities into their websites, mobile applications, customer experiences, and internal workflows. Potential examples include virtual makeup and eyewear applications, AI-generated employee headshots, customer-facing avatar tools, digital advertising platforms, personalized shopping experiences, and software that analyzes facial characteristics.

In many instances, the business deploying the application may have limited visibility into the technical processes performed by its AI vendor. An organization may know that its application generates a new image without understanding whether the vendor extracts facial geometry, creates biometric templates, retains facial representations, or uses uploaded photographs for model training. That information gap can create compliance challenges.

Whether a particular business faces liability will depend on its role in the processing, the relevant statutory requirements, and the facts surrounding the collection or receipt of the information. Merely using a third-party AI vendor does not automatically establish a BIPA violation.

However, relying on a vendor's technology does not eliminate the need to evaluate potential privacy obligations.

Vendor Agreements and AI Procurement Deserve Closer Attention

The litigation also underscores the importance of addressing biometric data processing during AI vendor selection, contracting, and ongoing oversight.

Traditional software agreements may not adequately describe how AI applications analyze uploaded images or what data they generate from those images. Businesses evaluating AI-powered image applications should consider whether their agreements and due diligence processes adequately address:

- **Biometric processing disclosures.** Vendors should clearly explain whether their technology creates or processes facial geometry scans, biometric templates, or other potentially regulated information.
- **Data ownership and permitted uses.** Agreements should identify how uploaded photographs and derived information may be used, including whether the vendor may use that information for model development, training, analytics, or other secondary purposes.
- **Retention and deletion.** Businesses should understand how long uploaded images and derived information are retained, whether deletion is technically supported, and whether applicable retention and destruction obligations can be satisfied.
- **Notice and consent responsibilities.** Contracts should allocate responsibility for determining and implementing required disclosures and obtaining legally sufficient releases.
- **Security and third-party access.** Agreements should address appropriate safeguards, subcontractor processing, access restrictions, and unauthorized disclosure of sensitive information.
- **Indemnification and insurance.** Organizations should evaluate whether contractual indemnities and available insurance coverage adequately address biometric privacy claims and regulatory investigations.

These considerations are particularly important where a vendor's functionality evolves through software updates, new model releases, or changes to its data processing practices.

Five Steps Businesses Should Consider Now

Businesses using or evaluating AI-powered image technologies should consider the following proactive measures.

1. **Inventory AI applications that process images or facial characteristics.** Identify customer-facing tools, employee applications, marketing technologies, and third-party integrations that collect or process photographs or videos of individuals.
2. **Evaluate the underlying processing activities.** Determine whether applications merely modify images or also extract facial geometry, generate biometric templates, or create other information potentially subject to biometric privacy laws. Technical documentation and vendor representations may be necessary to make this determination.
3. **Review notices, consent mechanisms, and retention practices.** Where regulated biometric processing occurs, assess whether the organization's disclosures, releases, retention policies, and deletion procedures satisfy applicable legal requirements.
4. **Reassess vendor contracts and data governance controls.** Confirm that agreements appropriately allocate compliance responsibilities, restrict unauthorized secondary uses, and address security, retention, and potential liability.

5. Incorporate biometric privacy into AI governance programs. Organizations should consider biometric processing as part of their broader AI risk assessments, procurement reviews, privacy impact assessments, and ongoing vendor monitoring.

These steps may help organizations identify compliance gaps before they become the subject of litigation.

Looking Ahead: Existing Privacy Laws Are Being Applied to New AI Technologies

The Grok lawsuits reflect a broader trend in privacy litigation: plaintiffs are increasingly seeking to apply existing statutory frameworks to emerging technologies and data processing practices.

Although BIPA predates the widespread adoption of generative AI, its requirements may apply to newer applications when the underlying technology performs activities covered by the statute.

The outcome of these cases could help clarify the circumstances under which generative AI image processing constitutes biometric collection. Until courts address those questions, businesses should avoid assuming that AI-generated images fall outside biometric privacy requirements simply because users voluntarily upload photographs or request image transformations.

The key issue is not necessarily what the application produces but what information it collects, derives, retains, or discloses in the process. For businesses, understanding how AI applications process personal information is becoming as important as understanding what those applications can do.

As AI capabilities continue to evolve, organizations that incorporate privacy compliance, vendor oversight, and responsible data governance into their technology decisions will be better positioned to manage emerging legal risks.

Shumaker's Technology, Data Privacy, Cybersecurity & Artificial Intelligence attorneys advise businesses on privacy compliance, AI governance, technology transactions, vendor risk management, and emerging litigation risks associated with the development and deployment of artificial intelligence.

This article is provided for informational purposes only and does not constitute legal advice.