ALM | LAW.COM

Six Tips for Managing Liability and Insurance for Facial Recognition and Other Biometric Technology

By Cort T. Malone

October 14, 2025

Companies across all sectors—from retail and hospitality to finance and healthcare—are deploying Facial recognition technology (FRT) and other biometric identification systems to enhance security, personalize customer experiences, and streamline business interactions.

Whether it's a fingerprint scan to clock in for a shift, a retinal scan to confirm access to secure areas, a "virtual try-on" tool for cosmetics, or a cashier-less checkout system that identifies customers as they shop, the applications are growing.

These technological leaps come with significant legal and financial risks. A patchwork of aggressive state and local laws has created a minefield of liability for businesses that collect, use, or store biometric data.

The most formidable of these is Illinois' Biometric Information Privacy Act (BIPA), the most stringent biometric privacy law in the country that includes a private right of action. Under BIPA, a business can be liable even without a data breach, as lawsuits under the statute often hinge on procedural missteps, such as failing to obtain proper written consent or not maintaining a publicly available data destruction policy.

Facial Recognition

As more states—including Texas, Washington, and California—and cities like New York and Portland, Oregon, enact their own biometric privacy regulations, the compliance and litigation landscape becomes ever more complex.

For any business using or considering FRT or other biometric technology, understanding these risks and implementing a proactive strategy to manage liability is essential for survival. This article outlines six tips for minimizing liability and maximizing the odds that your insurance policies will actually protect you when a claim based on the use of new technology inevitably arises.

1. Master the Consent and Notice Requirements in All Applicable Jurisdictions

Notice and consent are the cornerstones of compliance with most state regulations concerning

FRT and other biometric technology. Before a company collects any facial scan or other biometric data, BIPA requires that the company first: (i) inform the individual in writing that the data is being collected or stored; (ii) inform them in writing of the specific purpose and length of term for collection, storage, and use; and (iii) receive a written release executed by the person.

New York City's Biometric Identifier Information Act similarly requires businesses to post "clear and conspicuous" signage at all customer entrances notifying them that biometric data is being collected.

Simply burying consent in a lengthy, click-through terms-of-service document is a risky strategy that may not hold up in court. The consent should be explicit, informed, and separate from other terms. As Sephora discovered in a lawsuit over its virtual try-on tool, failing to meet these strict notice and consent requirements is one of the most common and easily avoidable sources of litigation.

2. Establish and Adhere to Publicly Available Data Policies

BIPA mandates that any private entity in possession of biometric data "develop a written policy, made available to the public, establishing a retention schedule and guidelines for permanently destroying" the biometric information it collects. The policy must specify when the data will be destroyed, which must be either when the initial purpose for collecting it is satisfied or within three years of the individual's last interaction with the company, whichever comes first.

These policies must be documented, they must be public, and companies must follow them. Failing to have or adhere to such a policy is a direct violation of BIPA and can form the basis of a lawsuit on its own.

3. Implement Robust Data Security Measures

Once a company lawfully collects biometric data, there is an ongoing duty to protect it. BIPA, for example, requires entities to store and protect all biometric information "using the reasonable standard of care within the private entity's industry," and in a manner that is at least as protective as how the company protects its other confidential and sensitive information.

Failing to secure biometric data properly significantly increases a company's risk. Because biometric identifiers like a faceprint or fingerprint are permanent and cannot be changed, a data breach involving this information is a catastrophic event for consumers, making businesses utilizing this technology prime targets for litigation, including class actions.

Strong cybersecurity measures, including robust encryption and well-tested incident response plans, are critical not only for compliance but also for securing favorable terms from your insurance carriers.

4. Test Systems for Accuracy and Fairness

Studies and regulatory bodies have raised concerns that FRT systems can be inaccurate and perpetuate biases based on race and gender. The National Association of Insurance Commissioners (NAIC), in a model bulletin adopted by 24 states as of June 2025, noted that AI systems present "unique risks to consumers, including the potential for inaccuracy, [and] unfair discrimination."

Using a biased system can lead to discriminatory outcomes, reputational damage, and new avenues for litigation and enforcement. As part of any company's due diligence, it should vet all third-party FRT vendors and, where possible, conduct its own testing to ensure the technology is fair and accurate for all individuals.

5. Diligently Review Your Insurance Coverage

When a lawsuit is filed, whether under BIPA or other privacy protection regulations, many businesses are shocked when their insurance companies deny the claim. While several types of policies may potentially offer protection—including Commercial General Liability (CGL), Employment Practices Liability (EPL), Directors and Officers (D&O), and standalone Cyber insurance – insurance companies often cite policy conditions and exclusions designed for other types of liability in an effort to avoid coverage.

Insurance companies have aggressively fought these claims in court, first relying on common exclusions in CGL and other liability insurance policies such as those for "Access or Disclosure of Confidential or Personal Information," "Recording and Distribution of Material in Violation of Law," and "Employment-Related Practices."

Policyholders initially found success defeating these exclusions in court, such as in the landmark *West Bend Mutual Ins. Co. v. Krishna Schaumburg Tan* decision where the Illinois Supreme Court found a duty to defend a BIPA claim under a CGL policy.

Insurance companies adapted by introducing even more restrictive exclusions specifically targeting the collection of data and violations of biometric privacy laws.

It is critical to work with knowledgeable insurance brokers to review your entire insurance portfolio, identify potential gaps, and negotiate the broadest possible coverage before a claim is made. And when a claim does occur, it is often beneficial to engage experienced coverage counsel early on to head off some of the typical insurance company efforts to avoid coverage.

6. Stay Informed on Regulatory Trends

The legal landscape for biometrics is evolving at breakneck speed. Many states, including New York, Arizona, and Hawaii, are considering BIPA-style legislation, and more are expected to follow.

Federal proposals like the American Privacy Rights Act (APRA) are under consideration, and SEC rules now require public companies to make timely disclosures about cybersecurity incidents, creating another layer of D&O liability risk. Staying informed about these trends is crucial for adapting your compliance programs and anticipating future risks.

Conclusion

The key to navigating the rapidly changing regulatory and legal environment in which biometric technology operates is a proactive strategy focused on rigorous compliance and diligent risk management.

By obtaining explicit consent, maintaining transparent data policies, ensuring robust security, and regularly reviewing your insurance coverage with brokers and counsel, you can mitigate the risk of devastating lawsuits and ensure your business is protected. In this high-stakes arena, an ounce of prevention is worth millions of dollars in cure.

Cort T. Malone *is a shareholder in Anderson Kill's New York and Stamford offices and co-chair of the firm's Biometric Liability Insurance Recovery Group.* **Anastasia Chupryna,** *a third-year J.D. candidate at Fordham University School of Law, assisted in the preparation of this article.*