POLICYHOLDER ADVISOR

November 11, 2025

Insurance Considerations for Claims Involving Facial Recognition and Other Biometric Technology

By Cort T. Malone

Facial recognition technology (FRT) and other biometric identification technologies are no longer science fiction; they are a rapidly expanding feature of the modern business landscape. Companies across a broad range of industries, including retail, hospitality, finance, and healthcare are deploying FRT and other biometric systems to enhance security, personalize customer experiences, and streamline business interactions. New applications are emerging constantly – witness the “virtual try-on” tool for cosmetics and cashier-less checkout systems that identify customers as they shop. With new uses come new liability risks – as suits against M.A.C. Cosmetics (for virtual try-on) and Amazon (for cashier-less checkout) illustrate.

I. Risks of Using FRT and Other Biometric Technology

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 utilized of these laws is Illinois’ Biometric Information Privacy Act (BIPA), which 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 logistical missteps, such as failing to obtain proper written consent or not maintaining a publicly available data destruction policy. In 2021, New York City passed a law similar to BIPA in providing a right of private action, albeit with a 30-day notice-and-cure provision. In recent years, other states including California, Texas, Virginia, and Washington have passed biometric privacy laws that do not contain a private right of action but are enforced by the state’s attorney general.

Navigating the legal risks of FRT and other biometric technology requires a proactive and multi-faceted approach. There are several practices that businesses can adopt to potentially reduce liability exposure and strengthen their position in the event of an insurance dispute over privacy claims. These practices include: (1) mastering the consent and notice requirements for use of FRT and biometric technology in all applicable jurisdictions; (2) establishing and adhering to publicly available data policies; (3) implementing robust data security measures; (4) testing technology systems for accuracy and fairness; and (5) staying informed on regulatory trends in these areas.

On this last point, companies must be aware that the legal landscape for FRT and 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 compliance programs and anticipating future risks.

II. Potentially Responsive Types of Insurance

In addition to undertaking the above pre-loss or pre-claim activities, perhaps the most important thing that a company using FRT or other biometric technology can do is to take stock objectively of their insurance policies that should respond to claims involving these technologies. Several types of policies may potentially offer protection from technology-based privacy claims including Commercial General Liability (CGL), Employment Practices Liability (EPL), Directors and Officers (D&O), Errors & Omissions (E&O), and standalone Cyber insurance.

With respect to cyber coverage, although there is no standard-form cyber policy, cyber policies typically include coverage for cyber security incidents, such as the improper safeguarding of personally identifiable information and potential unauthorized access by third parties. In the FRT and biometric information context, such coverage may be helpful if there is a data breach or security failure that makes personally identifiable information vulnerable to unauthorized access. Cyber policies are continuously evolving with the changing threat landscape, and while current cyber policies generally do not include FRT-related exclusions, this may change should liability exposure increase.

D&O coverage may respond to a variety of claims related to FRT or other biometric technology if the use of such tech results in discriminatory practices, violations of privacy laws, or other failures in adhering to regulations. Additionally, D&O policies can address derivative actions, where shareholders may sue directors and officers on behalf of the company for alleged misconduct including improper vetting or use of new technologies. Similarly, E&O insurance policies provide coverage for liabilities that arise from negligence in providing professional services. Specifically, technology E&O insurance aims to protect tech companies against risks associated with mistakes, negligence, or other failures associated with their tech products or services.

EPL insurance primarily provides coverage against employment claims made against employers by their employees. These policies typically cover wrongful employment practices such as allegations of discrimination, sexual and workplace harassment, wrongful termination, and retaliation. As biometrics tools become increasingly used in tracking, monitoring, and evaluating employees, there is potential for these tools to lead to allegations of discrimination. When employers use such systems to monitor employee productivity, employees may feel unjustly targeted, leading to hostile work environment claims. EPLI policies can cover defense or settlement costs for these types of claims.

III. FRT and Biometrics Claims and Insurance Company Response

FRT already has begun spawning lawsuits over its use under various statutory and common law privacy causes of action. These suits seek large damages awards such as those originally sought under BIPA before the Illinois legislature limited the damages recoveries available under that statute. Before that legislative change, however, the initial tidal wave of BIPA claims propelled a subsequent wave of coverage litigation.

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. As a result, 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.

In conclusion, facial recognition and other biometric technology offer powerful tools for businesses but also present added risk that may lead to a perilous legal and financial landscape. The proliferation of privacy laws means that no company can afford to be complacent. The key to navigating this environment is a proactive strategy focused on rigorous compliance and diligent risk management. Companies also must regularly review their insurance coverage with brokers and counsel to mitigate the risk of potentially devastating lawsuits.

Authors

Robert D. Chesler / *rchesler@andersonkill.com*
Bob is a shareholder in Anderson Kill's Newark office and is a member of the firm's Cyber Insurance Recovery Group. Bob represents policyholders in a broad variety of coverage claims against their insurers and advises companies with respect to their insurance programs.

ANDERSON KILL