Will Insurance Come to the Rescue in Biometric Data Handling Claims? New Privacy Laws Could Be Kryptonite for Liability Coverage

Major biometric damages claims are here to stay, and companies using biometric-based tech must watch out for new exclusions in their liability coverage.

By: Cort T. Malone and James Goodridge | June 15, 2023

Topics: Claims | Legal/Regulatory | Liability | Risk Insider

We are halfway through 2023, and it's already been another blockbuster year in the biometric litigation universe.

The main characters are back — the Illinois Biometric Information Privacy Act ("BIPA") and the justices of the Illinois Supreme Court. And the script has not changed much — a business scans workers' fingerprints or retina, a worker brings class action seeking hundreds of millions of dollars, and the business's insurance company disappears without a trace.

But thanks to a (dynamic) duo of decisions from Illinois' highest court, the stakes have never been higher. Adding to the complexity, the action is no longer contained to a single statutory scheme, as a new challenge to a previously untested law has arisen in New York City, and a potential new threat to companies lurks in the New York state legislature.

As for whether insurance might come to companies' rescue and save the day, courts thus far mostly have supported coverage for BIPA claims, but new policy exclusions are on the horizon. Policyholders must remain vigilant, look to their current insurance if exposed to liability, and consult experienced brokers and insurance counsel when renewing policies or obtaining new coverage.

Bigger Risks in Black (Horse) and White (Castle)

The Illinois Supreme Court delivered two much anticipated decisions earlier this year.

First, in Tims v. Black Horse Carriers, the Court held that all claims for violations under BIPA are subject to the state's five-year limitation period, based on the statute's text, the legislative intent, and the practical need for a single, workable limitation period. Then, in Cothron v. White Castle, the Court found that a BIPA claim accrues every time an individual's information is collected for purposes of calculating damages, not just on the first collection.

Together, the Black Horse and White Castle decisions have a host of implications for policyholders. At a minimum, the decisions are likely to result in more actionable cases against businesses and the demand for larger damages awards, as parties bring claims previously presumed to be time-barred and base their damages on a per-scan basis.

However, providing parties more time to bring a BIPA claim may allow policyholders to seek coverage under more policies than before. In other words, alleged violations looking back five years per the Black Horse ruling may allow policyholders to tap into older policies that span the time period of the alleged violations.

Of course, the availability of historical coverage will turn on the language of the policies. Positive changes negotiated during renewals could make more recent policies stronger vehicles for coverage, though older policies may be less likely to include biometric-specific exclusions.

Similarly, the larger damages figures — based on the per-scan mandate in White Castle — may entitle policyholders to reach further up their coverage towers to access umbrella and excess coverage.

Popular Stars Added to the Cast

A new story is being told in Manhattan, as Amazon became the latest major corporation to face litigation over its alleged use of biometrics. That case involves New York City's Biometric Privacy Law, which the municipality introduced last year in a revision to its administrative code.

The law applies to commercial establishments and prohibits businesses from collecting biometric identifiable information ("BII") — facial scans, fingerprints, etc. — without first posting a conspicuous sign at customer entrances. The signs must notify customers in plain and simple language how biometric identifiers are being collected or processed.

The law also prohibits covered companies from selling, leasing, trading, sharing, or otherwise profiting from that biometric information. Under the law, commercial establishments may face harsh penalties: up to $500 for each signage violation; up to $500 for each negligent sale violation; and up to $5,000 for each intentional or reckless sale violation.

Cort T. Malone, co-chair, biometric liability insurance recovery group, Anderson Kill

While the New York City law provides for a private right of action, it also provides a 30-day notice-and-cure provision, which likely has prevented the plethora of class-action lawsuits seen in Illinois.

The plaintiff in the Amazon case argues that Amazon ran afoul of the city's law by collecting biometrics of customers who entered its Amazon Go stores. Specifically, the plaintiff alleges that Amazon scans the body size and shape of all customers, regardless of whether they use a palm scanner to enter the store, and that Amazon fails to adequately warn customers of such collection.

Recently, Amazon moved to dismiss, primarily arguing that its "Just Walk Out" technology does not collect biometric information, and that the plaintiff lacks standing to bring his claims because he uses the Amazon App to enter the store, rather than the palm scanner.

To the first point, Amazon argues that the alleged body scanning is above board because the information collected does not contain "unique characteristics of any specific person." Rather, Amazon argues that such scans only register, for example, the approximate height and build of person, which can be used to differentiate customers in the store but is insufficient to specifically identify such person.

Regarding standing, Amazon argues that the plaintiff's only alleged injury resulted from his failure to read the App's privacy policy when he used it to enter the store.

The Sequels Are Coming

Back in January 2021, a group of New York State legislators introduced a bill for the "Biometric Privacy Act," (the "BPA") which bears a strong resemblance to Illinois' BIPA in form and substance.

In short, New York State's BPA — reintroduced in February 2023 as S04457/A01362 — would cover similar information as BIPA, and would impose similar requirements. For example, the BPA would define "biometric identifier" as "a retina or iris scan, fingerprint, voiceprint, or scan of hand or face geometry," and would include a carveout for information collected for health care treatment.

Like its Illinois counterpart, NY's BPA would require businesses to establish a written policy setting forth a schedule and guidelines for permanently destroying people's biometric identifiers and biometric information — either when the initial purpose for collecting or obtaining such identifiers or information has been satisfied, or within three years of the individual's last interaction with the private entity, whichever occurs first.

James A. Goodridge, attorney, Anderson Kill

Like the NYC Biometric Privacy law, the BPA would include a private right of action, and preclude the sale, lease, trade, or otherwise profiting from the use of biometric information or identifiers. But crucially, unlike the city's law, the state's BPA, as currently drafted, contains no cure provision.

The BPA could be game changing. Without a cure provision, enterprising plaintiffs would not have to wait for companies to attempt to fix alleged violations. This could lead to the same massive upswing in lawsuits in New York that occurred in Illinois, along with potentially comparable multi-million-dollar damages awards.

Other states, such as California, Texas, Virginia, and Washington have passed biometric privacy laws that do not contain a private right of action, but rather are enforced by the state's attorney general.

But companies in states with biometric privacy laws that do not include a private right of action still should be concerned, as state attorneys general have aggressively pursued violations. Most notably, the Texas Attorney General is pursuing claims against Meta,

Facebook's parent company, that could result in billions of dollars' worth of damages under the state's Capture or Use of Biometric Identifier Act ("CUBI").

Many other states across the nation are considering bills on biometric privacy protection as well.

Insurance Recovery Kryptonite

As more state biometric privacy laws are passed, the risks for companies using BII continue to grow. More BII liability risk means more insurance coverage disputes are sure to follow. So far, insurance companies' attempts to deny coverage for biometric claims on the basis of existing exclusions in liability policies — e.g., exclusions pertaining to disclosure of confidential information and employment related acts — have mostly failed.

But insurance companies, noting the spate of large awards and settlements, are beginning to introduce more specific exclusions into general liability and employment practices liability policies.

When purchasing and renewing insurance policies, businesses at risk of liability under biometric privacy laws need to scrutinize their existing liability coverage and be wary of insurance companies adding such exclusions or making other impactful changes to policy language that may endanger coverage for biometric privacy claims.

Because biometric-based technology continues to proliferate, blockbuster biometric damages claims are here to stay. Accordingly, policyholders — especially those conducting business in Illinois and New York — must take careful stock of both their current and potential future uses of biometrics, and carefully review their insurance policies (both current and renewal) to maximize protection against biometric privacy law claims and deal with insurance companies seeking to avoid the resulting potential liability. **&**

Cort T. Malone is a shareholder in the New York office of Anderson Kill and co-chair of the firm's biometric liability insurance recovery group. James A. Goodridge is an attorney in Anderson Kill's New York office who focuses his practice on insurance recovery and commercial litigation.