Corporate Counsel Business Journal

May • June 2021
CCBJournal.com

CCBJ

Managing Risk of Liability Stemming from Biometric Tech and Privacy Laws

CORT MALONE, ROBERT CHESLER, AND JAMES GOODRIDGE
ANDERSON KILL

▶ Using biometrics may increase efficiency, but companies that do so should also be careful to avoid – and insure against – liability.

Biometric technology is here, and its use will only continue to grow in the coming years. As a result, litigation under privacy laws protecting individuals' biometric information has exploded. Such litigation will likewise continue to grow, as evidenced by the activity of the past few months.

In January, a group of New York state legislators introduced a biometrics regulation bill that contains a private right of action similar to the already enacted Illinois Biometric Information Privacy Act (BIPA).

In February and early March, four major developments occurred regarding BIPA litigation. First, a California District Court approved Facebook's $650,000,000 biometrics settlement.

Second, the popular music video app Tik-Tok agreed to pay $92,000,000 in a biometrics settlement of BIPA claims, though approval of the settlement has been delayed until at least April 6, in light of claims that the settlement's value is "embarrassingly low." *In re TikTok Inc. Consumer Privacy Litigation*, 1:20-cv-04699, (N.D. Ill 2020).

Third, Holiday Inn was sued in Illinois by its own insurance company for making a coverage claim for a biometric class action. *AXIS Surplus Insurance Co. v. New Crown Holdings LLC*, case number 2021CH00900.

Biometric regulation centers on the individual's right to control his or her personal information.

Fourth, on March 3, a college student initiated a class action against DePaul University over its use of facial-recognition technology in online exam proctoring.

The above are just a few examples of the burgeoning class of litigation over the use of biometrics. And as the N*ew Crown* case demonstrates, there will be additional litigation over the extent to which insurance covers these claims, particularly as more states ratify laws providing a private right of action for biometric privacy violations.

Background on Biometrics

Biometrics is the use of personal identifiers such as fingerprints and retina scans to identify people. These identifiers are unique and reliable. A company may require its employees to check in and out with a fingerprint scan rather than a time clock. In *Rosenbach v. Six Flags*, 129 N.E.3d 1197, 1205 (Ill. 2019), a Six Flags amusement park required a thumb print in order to obtain a season pass and was sued for failing to meet the BIPA disclosure requirements described below. The technology continues to develop and expand. For example, the travel hub country Dubai is in the process of rolling out an iris scanner that verifies one's identity and eliminates the need for any human interaction when entering or leaving the country.

The particular problem for companies in the use of biometrics is exemplified by Illinois' enactment of BIPA. Illinois is not the only state that regulates biometrics, but it is the only state currently whose biometric statute includes a private right of action. The penalty for a violation is $1,000, with an increase to $5,000 if the violation is reckless or intentional. A plaintiff need not show any injury from the violation – just the violation itself. As a result of these features, BIPA has made Illinois a center for biometric class action litigation.

Biometric regulation centers on the individual's right to control his or her personal information. Unlike a stolen credit card or driver's license, a person's biometric data cannot be simply canceled or replaced. Companies must advise individuals that they are collecting biometric information, indicate the length and purpose of the collection, and obtain the individual's written consent to proceed with the collection. Certain covered entities are prohibited from selling or profiting from the information and must use reasonable standards of care in safeguarding the information.

Several Types of Insurance May Cover Biometric Claims

In the face of liability for biometric claims, companies have turned to their insurance companies, only to be met by a solid wall of denial. The key insurance concept involved is invasion of privacy. Several different types of policies may provide invasion of privacy coverage, including general liability, employment practices, directors and officers, and cyber.

General Liability Insurance

The Personal and Advertising Injury Coverage within general liability policies includes coverage for invasions of privacy. This insurance applies to "personal injury," which typically is defined as "injury, other than 'bodily injury,' arising out of … [o]ral or written publication of material that violates a person's right of privacy."

West Bend Mutual Ins. Co. v. Krishna Schaumburg Tan, 2020 IL App (1st) 191834, *appeal allowed*, 154 N.E.3d 804 (Ill. 2020) is the only case so far construing this provision in the context of biometrics. In that case, a customer accused a salon of violating BIPA by storing and distributing patrons' fingerprint data without their consent. The policyholder sought coverage under a provision covering personal injury claims arising from the publication of information that violates an individual's privacy rights. *West Bend* argued that "publication" required disclosure to the public at large, not just to a single third-party vendor. The appellate panel disagreed and found coverage. The case now sits before the Illinois Supreme Court, with a decision expected soon.

Employment Practices Liability Insurance

Biometric measures regularly are used in various work environments, and employees have filed biometric claims. For example, the Salvation Army recently agreed to pay

approximately $898,000 to settle a class action surrounding its practice of having its employees log their fingerprint when clocking in and out.

Companies should have employment practices liability insurance (EPLI), which offers coverage for a broad range of employment torts. Around 60 percent of existing EPLI policies provide coverage for invasion of privacy, which should respond to biometric claims.

Directors and Officers Insurance

Biometric claims may trigger coverage under directors and officers (D&O) policies. While public company D&O policies typically only cover securities claims against the entity, directors and officers may be covered when sued for failing to oversee operations that resulted in biometric violations.

Private company D&O policies also provide entity coverage that conceivably covers biometric claims. Thus, both public and private company policyholders should investigate D&O coverage should they be faced with biometric claims.

Cyber Insurance

A robust and properly designed cyber insurance policy may afford the policyholder coverage for a BIPA complaint. Currently, there is not a standalone cyber policy specifically

BIPA has made Illinois a center for biometric class action litigation.

designed to address BIPA claims. However, regulatory fines and penalties, like those that could be issued under BIPA, could potentially be covered in the Bermuda market using a manuscript fines and penalties policy form.

Exclusions

The insurance industry has developed several exclusions for coverage related to liability for disclosure of personally identifying information, and it would not be surprising to see more such exclusions going forward. For example, in *West Bend*, the insurance company sought to enforce its exclusion for claims resulting from the violation of statues or regulations that prohibit or limit the "sending, transmission, communicating or distribution of material or information."

In *New Crown*, the general liability policy excluded coverage for damages arising from "[a]ny access to or disclosure of any person's or organization's confidential or personal information, including patents, trade secrets, processing methods, customer lists, financial information, credit card information, health information or any other type of nonpublic information[.]" While a few biometric cases involve disclosure – like *West Bend* and *New Crown* – most chiefly implicate a failure to obtain consent, so these disclosure-based exclusions would not apply.

Policyholders should be aware of these exclusions as they renew or place coverage, especially if they already use, or plan to use, biometrics. Because the use and regulation of biometrics is certain to increase in the coming months and years, companies must evaluate their insurance policy options to ensure coverage for biometric claims. ■

Cort Malone is a shareholder in the New York office of Anderson Kill P.C. He focuses his practice on insurance coverage litigation and dispute resolution, with an emphasis on commercial general liability insurance, directors and officers insurance, employment practices liability insurance, advertising injury insurance, and property insurance issues. Reach him at cmalone@andersonkill.com.

Robert Chesler is a shareholder in the Newark, NJ office of Anderson Kill P.C. He represents policyholders in a broad variety of insurance coverage claims and advises companies with respect to their insurance programs. Reach him at rchesler@andersonkill.com.

James Goodridge is an associate (pending admission) in the New York office of Anderson Kill P.C. He focuses his practice on corporate and commercial litigation, employment law and insurance recovery, exclusively on behalf of policyholders. Reach him at jgoodridge@andersonkill.com.