New York Law Journal

NEW YORK LAW JOURNAL SPECIAL REPORT

An ALM Publication

Cybersecurity

WWW.NYLJ.COM

VOLUME 265—NO. 38

MONDAY, MARCH 1, 2021

Insurance Coverage For Violations of Biometric Privacy Acts

BY CORT MALONE, MARC SCHEIN, ROBERT CHESLER AND JAMES GOODRIDGE

SHUTTERSTOCK

On Jan. 6, 2021, a bipartisan group of 17 New York legislators introduced a biometrics bill in the New York Legislature modeled on the Illinois Biometric Information Privacy Act (BIPA). Biometrics are personal identifiers such as retina scans, fingerprints, and voice or face recognition. They are individualized and reliable, and increasingly used for security and computer and systems access. BIPA, which creates a host of obligations for collectors of biometric data and a private right of action for individuals harmed by violations, has been a disaster for Illinois businesses, resulting in literally hundreds of class actions.

The New York bill contains the same provisions from BIPA that created this litigation tsunami, as it similarly would regulate the use, and abuse, of biometric information. Companies subject to the bill must advise individuals that the companies are collecting biometric data, indicate the length and purpose of the collection, and obtain written permission to proceed. Covered entities are prohibited from selling or profiting from this information, must use "reasonable" standards of care, cannot disclose the information except in enumerated circumstances, and must develop a written retention policy. The bill comes just over a year after New York made biometric information a data element subject to the state's data breach notification laws under the SHIELD Act.

The provisions that have caused the litigation rush are those that created

CORT MALONE *is a shareholder in the New York office of Anderson Kill P.C. and a member of the firm's insurance recovery group.* MARC SCHEIN *is co-chair of the Cyber Center of Excellence at Marsh & McLennan Agency.* ROBERT CHESLER *is a shareholder in the Newark office of Anderson Kill P.C. and a member of the firm's insurance recovery group.* JAMES GOODRIDGE *is an associate (pending admission) in the New York office of Anderson Kill P.C. and a member of the firm's insurance recovery group.*

a private right of action and imposed statutory damages of $1,000 per violation and $5,000 if intentional or reckless. Moreover, the Illinois Supreme Court has held that the plaintiff in a BIPA case need not show any actual injury—just a violation of the statute. *Rosenbach v. Six Flags*, 129 N.E.3d 1197, 1205 (Ill. 2019).

Rosenbach is instructive. In that case, Six Flags required a thumb scan to obtain a season pass. The plaintiff asserted that Six Flags did not: (1) inform customers in writing that the data would be collected; (2) explain in writing the purpose of the collection; or (3) obtain written consent before collecting. The court held that the plaintiff did not need to show any adverse impact, just a statutory violation. It is likely that Six Flags had required thumb scans of hundreds if not thousands of individuals. At $1,000 per violation, the lure of these cases for plaintiffs' lawyers is only too obvious.

The Ninth Circuit reached a similar conclusion in a BIPA claim. *Patel v. Facebook*, 932 F.3d 1264 (9th Cir. 2019), cert. denied, 140 S. Ct. 937 (2020). In *Patel*, the plaintiff sued Facebook for its use of facial recognition software without the consent of the users. The court found that there was either actual harm or a material risk of harm to privacy interests. Facebook settled for $550,000,000.

As companies reeled from BIPA liability, they turned to their insurance for redress, only to be met by a solid wall of coverage denials. But insurance coverage for BIPA liability may exist under several different types of policies: general liability; directors' and officers'; employment practices; and cyber.

General Liability Insurance

The only reported decision to date on insurance coverage for biometric liability arose under a general liability policy. *West Bend Mutual Ins. Co. v. Krishna Schaumburg Tan*, 2020 IL App (1st) 191834, appeal allowed, 154 N.E.3d 804 (Ill. 2020). The policyholder in that case sought coverage under the policy provision providing coverage for liability arising out of "written publication of material that violates a person's right of privacy." The policyholder had provided customers' fingerprint data to a vendor. The insurance company argued that no "publication" had occurred because that term required dissemination to a wide audience. The court disagreed, holding that "publication" was also commonly understood to encompass a more limited sharing with a single party, and found coverage.

Directors' and Officers' Insurance

Directors' and officers' (D&O) insurance may apply to biometric claims. Public company D&O policies typically provide coverage for the entity for securities claims, which could include claims that, for example, the company failed to disclose in its SEC filings that it was subject to potential liability for biometric violations. Public company D&O policies also should apply to cover directors and officers facing lawsuits arising from company biometric violations. Such a suit might allege that the value of company stock fell because of biometric violations, and that the directors and officers failed to oversee corporate operations that resulted in the 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.

Employment Practices Liability Insurance

Biometrics have widespread use in the workplace, and employee biometric claims have occurred. Many manufacturers require employees to use their fingerprints to clock in. Similarly, warehouses often require truck drivers to scan their fingerprints when picking up or delivering loads. In one case, a former employee brought an action alleging that his employer violated BIPA by requiring employees to use a biometric scanner without obtaining their written permission. The employer asserted that it had deleted the data after it stopped using the technology in Illinois. The court recently approved a settlement involving the estimated class of employees.

Similarly, in a case involving the Salvation Army, a former employee alleged that the organization violated BIPA by requiring employees to log their fingerprint or other biometric information when clocking in and out. The employee further alleged that the organization neither obtained written consent nor disclosed whether and how the information would be stored or used. The Salvation Army has agreed to pay approximately $898,000 to settle the class action.

General liability policies typically exclude claims by employees. However,

companies should have employment practices liability insurance (EPLI), which offers coverage for a broad range of employment torts. Usually, EPLI policies provide coverage for invasion of privacy, which should be relevant to biometric claims.

Cyber Insurance

The cyber insurance marketplace has more than doubled in the last five years. According to Marsh & McLennan, in 2014 roughly 19% of its clients procured standalone cyber insurance. In 2019, that number had increased to 42%. The cyber marketplace is expected to grow by nearly 20% in 2021, according to Finaria. The cyber insurance policy forms are non-ISO, thus creating meaningful nuance in the policy language.

While the cyber insurance marketplace continues to be challenging, it is becoming common practice for insurers to cut their capacity, although astute cyber brokers are still getting deals done and done well. Several carriers have started to sublimit or exclude coverages in order to maintain profitable cyber books of business. Several insurers have exited the cyber marketplace altogether as claims continue to rise in frequency and severity.

How will a cyber insurance policy respond to a BIPA complaint? As with most answers in insurance, it depends. A robust cyber insurance policy designed properly may afford the policyholder coverage. One key component that policyholders should try to negotiate out of their cyber policies to ensure that coverage would apply is the data breach trigger. Currently, there is not a standalone policy specifically designed to address BIPA claims. However, regulatory fines and penalties, like those that could be issued under BIPA could be potentially covered in the Bermuda market using a manuscript fines & penalties policy form.

Exclusions

The biggest hurdles for companies seeking insurance coverage for biometric liability, under any type of policy are the many exclusions added by insurance companies in recent years to policies for disclosure of confidential information and data-related liability.

For example, in one case in which a policyholder sued its insurance company for BIPA liability under the "invasion of privacy" coverage, the insurance company relied on an exclusion for claims arising from violations of a statute that "addresses, prohibits or limits the printing, dissemination, disposal, collecting, recording sending, transmitting, communicating or distribution of material or information" to deny coverage.

In another case brought under an EPLI policy, the insurance company relied on an "Access to or Disclosure of Confidential or Personal and Data-related Liability" exclusion, which denied coverage for "[d]amages arising out of (1) [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 non-public information; or (2) the loss of, loss of use of, damage to, corruption of, inability to access, or inability to manipulate electronic data."

Policyholders should be aware of these exclusions as they renew or place coverage, especially if they already use, or plan to use, biometrics.

As companies reeled from BIPA liability, they turned to their insurance for redress, only to be met by a **solid wall of coverage denials.** But insurance coverage for BIPA liability may exist under several different types of policies: general liability; directors' and officers'; employment practices; and cyber.

Conclusion

While the New York bill has not yet been enacted, it does bear striking similarities to BIPA. If the litigation maelstrom in Illinois serves as an example, New York business owners should be wary of potential exposure should the bill ultimately become law.