King & Spalding
Client Alert

AUGUST 16, 2019

For more information, contact:

Meghan Magruder
+1 404 572 2615
mmagruder@kslaw.com

Anthony P. Tatum
+1 404 572 3519
ttatum@kslaw.com

Shelby S. Guilbert, Jr.
+1 404 572 4697
sguilbert@kslaw.com

Joseph M. Englert
+1 404 572 3536
jenglert@kslaw.com

King & Spalding

Atlanta
1180 Peachtree Street, NE
Atlanta, Georgia 30309-3521
Tel: +1 404 572 4600

Biometric Data Regulations: Do Your Insurance Policies Cover This Emerging Risk?

Over the past several years, commercial use of biometric data has become increasingly prevalent. In response, several states have adopted biometric data privacy legislation. Consequently, companies that rely on biometric data face new regulatory risks, in addition to increased legal exposure to individual and class action lawsuits. In fact, the Ninth Circuit Court of Appeals recently affirmed certification of a class action alleging Facebook's face-scanning practices violate Illinois' biometric privacy law, finding that the class alleged sufficiently concrete injuries based on Facebook's alleged use of facial recognition technology without users' consent to establish standing. Insurance policies currently available on the market, including cyber insurance policies, may not adequately cover these risks. Therefore, companies collecting, utilizing, maintaining, distributing, and/or destroying biometric data should review their policies carefully to determine changes could be made to address potential coverage gaps.

BACKGROUND

What is Biometric Data?

Biometric data refers to measurable human physical or behavioral characteristics that are used to detect or authenticate individual identity. It includes voice prints, fingerprints, facial recognition, retina scans, iris scans, and/or hand geometry recognition.

How is Biometric Data Used?

Employers frequently use biometric data to track employee attendance and time, provide secure access to buildings or equipment, and to ensure secure login to computers and mobile devices. Businesses ranging from airlines to telecom companies to technology companies to even amusement parks increasingly collect biometric data to deliver services to their customers, or to provide alternatives to traditional password authentication.

New Laws Regulating the Use of Biometric Data.

While biometric data has many beneficial applications, it also presents legal risks. Illinois, Texas, and Washington have enacted laws regulating biometric data.[1]

Illinois Biometric Information Privacy Act[2]

Illinois is generally considered to have the most stringent state law concerning biometric data. Under the Illinois Biometric Information Privacy Act ("BIPA"), a private entity must (1) provide written notice to employees, (2) obtain written consent, and (3) make specific disclosures concerning the purpose and duration of data collection, storage, or use before collecting, storing, and using biometric data. Covered entities are prohibited from selling or profiting from collected data and are required to protect the data using reasonable standards of care as defined within their respective industries. Only in specific enumerated circumstances are entities allowed to disclose the data. Covered entities must also develop a written policy concerning the retention and destruction of biometric data that is compliant with the guidelines set forth in the statute. Notably, Illinois law permits a private right of action for technical violations with statutory damages of $1,000 per violation or $5,000 per intentional or reckless violation. Recovery of attorneys' fees is also allowed.

Individuals are not required to prove actual harm when bringing a suit under BIPA.[3] In *Rosenbach v. Six Flags Entertainment Corporation*, a 14-year-old student visited a Six Flags amusement park on a school field trip. As a part of the sign-up process to obtain a season pass, the student was required to scan his thumb into the Six Flags biometric data capture system. His thumbprint and season pass would subsequently allow him to enter the amusement park. The student's mother sued Six Flags on behalf of her son under BIPA claiming that Six Flags had unlawfully collected his biometric data without (1) informing him or his guardian in writing that the data would be collected, (2) explaining the purpose in writing of such data collection, and (3) obtaining written consent before collection. The mother did not allege any additional injury or harm other than a technical violation of the regulation. Nevertheless, after analyzing the legislature's intent, the Supreme Court of Illinois held that the mother's alleged injury was sufficient to maintain a claim under the biometric data statute. The Court explained that when a private entity does not comply with the statutory requirements laid out in BIPA, it results in an impairment, invasion, or denial of statutory rights. Thus, the individual whose biometric data was unlawfully collected, stored, or used is an "aggrieved person" entitled to seek recovery and need not plead additional consequences or harm.

Earlier this month, the Ninth Circuit Court of Appeals reached a similar conclusion when it affirmed certification of a class action based on the allegation that Facebook violated BIPA when it developed and used facial recognition software without users' consent.[4] In *Patel v. Facebook, Inc.*, the class representatives alleged their privacy rights were violated under BIPA when, after they uploaded photos to Facebook, Facebook created and stored face templates for each of the plaintiffs without the required consent under BIPA. Facebook contended that plaintiffs lacked standing because they had merely alleged a "bare procedural violation of BIPA rather than injury to a concrete interest." However, the Ninth Circuit held that the plaintiffs had alleged a concrete and particularized harm, sufficient to confer Article III standing, because BIPA protected the plaintiffs' concrete privacy interest, and Facebook's development of a face template using facial-recognition technology without consent actually harmed or posed a material risk of harm to those privacy interests. This holding, along with the *Rosenbach* decision, establish that a plaintiff need not allege harm beyond the collection of biometric data without consent to state a claim under BIPA.

Texas Capture or Use of Biometric Identifier Act[5]

Under the Texas Capture or Use of Biometric Identifier Act, a private entity must (1) provide notice and (2) obtain consent from a data subject before collecting and using his or her biometric data for a "commercial purpose." This statute does not mandate that notice and consent be in writing nor does it stipulate specific disclosure requirements. Like the Illinois law, the Texas law prohibits the sale and disclosure of biometric data with limited exceptions and requires the

protection of biometric data using reasonable standards of care. Unlike Illinois law, Texas law does not provide for a private right of action. Instead, only the state attorney general may bring actions for violation of the Capture or Use of Biometric Identifier Act, with a maximum recovery of $25,000 for each violation.

Washington's Biometric Data Statute[6]

Washington's biometric data statute is similar to the Texas statute. First, like the Texas statute, Washington's statute requires notice and consent but does not explain the type of notice and consent necessary for compliance. It states that determination of compliance is context-dependent. Second, the Washington statute also limits regulation of biometric data to data collected and used for a "commercial purpose." It expressly excludes biometric data collected for security and law enforcement purposes. The Texas statute, however, does not define commercial purpose. Third, the Washington statute does not provide individuals a private right of action.[7] Fourth, it bans the sale, lease, or disclosure of biometric data with enumerated exceptions and requires the protection of biometric data using reasonable care. Notably, however, the Washington statute more narrowly defines the regulated biometric data[8] and does not include hand or face geometry.

Other States' Statutes

Bills proposing similar legislation are pending in Alaska, Connecticut, Massachusetts, Montana, and New Hampshire. Other state legislatures may look to Illinois, Texas, and Washington as models when enacting new legislation.

POTENTIAL GAPS IN INSURANCE COVERAGE FOR BIOMETRIC DATA LAW VIOLATIONS

Cyber Liability Insurance

Cyber liability policies generally provide coverage for costs arising from the unauthorized disclosure of personal consumer data, but still may not provide comprehensive coverage for violation of the new biometric data laws. Most cyber liability policies cover claims arising from "privacy events." A privacy event is often defined to include the unlawful or unauthorized disclosure of confidential or private information resulting from a breach of the policyholder's network, and may not extend to the unauthorized collection or use of such data. Thus, violations of biometric data laws based on the unauthorized *collection, storage, or other use* of the data may not be covered. Further, some cyber liability policies may define "confidential" or "private" data in a way that excludes or limits coverage for biometric data. Some policies also limit or exclude coverage for claims arising under specific, enumerated statutes. Courts have not generally ruled on whether such policies must cover biometric data law violations.

Commercial General Liability Insurance

Commercial or comprehensive general liability ("CGL") coverage protects companies from a broad range of claims resulting in "bodily injury," "advertising injury" or "property damage." However, CGL policies may not cover violations of biometric data privacy laws. While some courts have found coverage for data breach claims under CGL policies[9] most CGL policies now include endorsements that exclude or limit coverage for cyber related claims involving "electronic data." In 2014, the Insurance Services Office, Inc. ("ISO") crafted form language that specifically excludes or limits coverage for damages arising out of (1) "[a]ny access to or disclosure of any person's or organization's confidential or personal information" and (2) "[t]he loss of, loss of use of, damage to, corruption of, inability to access, or inability to manipulate electronic data."[10] This exclusion is now routinely added to CGL policies.

Courts also have not considered the question of whether biometric data qualifies as "electronic data," and is therefore subject to electronic data exclusions that are increasingly common in CGL policies. Electronic data is defined in ISO form endorsements as "information, facts or programs stored as or on, created or used on, or transmitted to or from computer software, including systems and applications software, hard or floppy disks, CD-ROMs, tapes, drives, cells,

data processing devices or any other media which are used with electronically controlled equipment."[11] While arguably "biometric data" is not "electronic data," courts so far have not considered this question.

Directors' and Officers' Liability Insurance and Errors & Omissions Liability Insurance

Coverage for violations of biometric data regulations may also be found under directors' and officers' ("D&O") and errors and omissions ("E&O") liability insurance policies that provide broad coverage for claims arising out of "wrongful acts" of the company and/or its officers and directors. However, like CGL policies, many D&O and E&O policies now often include "invasion of privacy" or "data breach" exclusions, which may limit insurance coverage for biometric data law violations.[12]

RECOMMENDATIONS

Companies that use or collect biometric data should review the terms and conditions in their cyber, CGL, D&O, and E&O insurance programs to determine if there may be additional enhancements that could be added to address the emerging risk from violation of biometric data legislation, including:

1. Ensure that biometric data is included in cyber liability policy definitions of data and/or confidential information.
2. Modify cyber liability policies to provide coverage for claims arising from the collection, storage, or use of biometric data. Include such treatment of biometric data in the definition of a privacy event.
3. Review policies carefully for exclusions for liabilities arising under emerging laws regulating the use of biometric data.
4. Carefully review cyber, CGL, and D&O policies at annual renewals to avoid coverage gaps.

We work closely with our clients and their risk managers to navigate developing data privacy legislation and to improve the wording of their cyber policies. We have helped our clients recover hundreds of millions of dollars in losses arising from cybersecurity and data breach incidents. Our Cyber Insurance Coverage Recovery practice works closely with our Data, Privacy & Security Practice, which has unparalleled experience in areas ranging from providing regulatory compliance advice, to responding to security incidents including data breaches and cybersecurity incidents, interfacing with stakeholders and the government, engaging in complex civil litigation (such as class actions), handling state and federal government investigations and enforcement actions, and advocating on behalf of our clients before the highest levels of the state and federal government.

[1] Insurance Coverage Disputes (LJP) § 1.04.
[2] 740 ILCS 14/15.
[3] *Rosenbach v. Six Flags Entm't Corp.*, 2019 IL 123186.
[4] *Patel v. Facebook, Inc.*, No. 18-15982, 2019 WL 3727424 (9th Cir. Aug. 8, 2019)
[5] Tex. Bus. & Com. Code § 503.001.
[6] Wash. Rev. Code Ann. § 19.375.020.
[7] Wash. H.B. 1493 § 4(2).
[8] The Washington statute only applies to "enrolled" biometric data. Covered entities enroll biometric data if they "capture a biometric identifier of an individual, convert it into a reference template that cannot be reconstructed into the original output image, and store it in a database that matches the biometric identifier to a specific individual." Wash. Rev. Code Ann. § 19.375.010.
[9] *See, e.g., Travelers Indem. Co. of Am. v. Portal Healthcare Sols., L.L.C.*, 644 F. App'x 245 (4th Cir. 2016)
[10] ISO Form CG 21 06 05 14 (2014).
[11] See Appendix of Forms, ISO CG 00 01 04 03 Commercial General Liability Coverage Form Exclusion 2.p.
[12] "The Internet of Buildings": Insurance of Cyber Risks for Commercial Real Estate, 71 Okla. L. Rev. 397, 440.