THOMSON REUTERS
PRACTICAL LAW™

Insurance Coverage for Biometric Data Privacy Claims

by Tae Andrews, Miller Friel PLLC, with Practical Law Data Privacy Advisor

Status: **Maintained** | Jurisdiction: **United States**

This document is published by Practical Law and can be found at: **us.practicallaw.tr.com/w-031-3339**
Request a free trial and demonstration at: **us.practicallaw.tr.com/about/freetrial**

This Practice Note provides an overview of the types of insurance policies that should provide coverage for costs associated with alleged and actual violations of biometric data laws, discusses potential coverage disputes, and offers best practices for organizations seeking coverage for biometric data-related claims.

Biometric data includes an individual's unique biological and physical characteristics, such as retina and iris scans, fingerprints, voice prints, facial scans, and hand geometry. Organizations nationwide increasingly use biometric identifiers for various reasons, such as authentication, monitoring, timekeeping, and other purposes uniquely suited to these human markers.

In response, several states have adopted laws regulating the collection, use, retention, and disclosure of biometric data. Companies that rely on biometric data now face regulatory risks and under at least one statute, private lawsuits.

Laws governing biometric data have also created an emerging frontier in insurance disputes and litigation over coverage for biometric data privacy claims. In some cases, insurers agree to defend under a reservation of rights, meaning that they intend to provide a temporary defense while actively working behind the scenes to dispute coverage. Insurers may also deny coverage outright and file a declaratory judgment action seeking a court determination that they do not need to provide the requested coverage.

This Note provides an overview of the types of insurance policies that may provide coverage for biometric data claims and costs, analyzes potential coverage issues under those policies, and offers best practices for policyholders seeking coverage for these claims and costs.

Corporate Uses for Biometric Data

Biometric technology has evolved significantly in recent years. Biometric data is now as easy to use as username and password combinations for verification and security purposes, among other uses.

Some of the most common uses for biometric data technology include:

- **Facial recognition technology.** Many online and social media platforms use biometric technology to instantly identify individuals by their photographs.
- **Tracking health and fitness information**. Companies now sell wearable accessories that automatically monitor and track various personal biological characteristics, including heart rate, step counts, and sleep time.
- **Consumer authentication for transactions**. Many consumer-facing organizations, such as retailers and banks, rely on biometrics-based user authentication to complete financial transactions and verify a customer's payment.
- **Enhancing corporate security**. Organizations increasingly use biometric technology for internal operational security purposes, such as:
  - retina and hand scanners in data centers and other highly secured areas; and
  - collecting and maintaining fingerprints for background investigations.
- **Timekeeping for employees.** This includes using fingerprints or hand scans to punch in and out on biometric timeclocks, to avoid time theft and "buddy punching."
- **Accessing employer-provided workplace equipment.** This includes accessing computer systems, copiers, and applications on laptops, tablets, and smartphones using facial recognition or fingerprint technology.

Because individuals generally cannot change their biometric data, access to that data presents different

policy and security concerns than conventional security information, such as login information and passwords. Several states have adopted laws governing the collection, use, storage, and disclosure of biometric data to address these risks.

Biometric Privacy Statutes

Several US states have enacted statutes focused specifically on biometric data collection requirements, including:

- The Illinois Biometric Information Privacy Act (BIPA) (740 Ill. Comp. Stat. 14/5).
- Texas' Capture or Use of Biometric Identifier Act (CUBI) (Tex. Bus. & Com. Code Ann. § 503.001).
- Washington State's law regarding biometric identifiers (RCW 19.375.010 to 19.375.900).

Other states regulate biometric data in their general privacy laws or in data breach notification laws (see, for example, California Consumer Privacy Act of 2018 (Cal. Civ. Code §§ 1798.100 to 1798.199); Virginia Consumer Data Protection Act (Va. Code Ann. §§ 59.1-571 to 59.1-581)). For information on data breach notification laws that include biometric data in definition of personal information, see Practice Note, State Data Breach Laws Protected Personal Information Chart: Overview.

While the statutory requirements and restrictions differ in laws regulating biometric data, common themes include:

- Requiring some form of notice:
  - that the entity collects biometric information; and
  - about how the entity uses the information.
- Requiring clear consent from the individuals to use their biometric data, sometimes in writing.
- Restricting to various degrees the sale, lease, or other disclosure of biometric information.
- Providing standards for confidentiality, retention, and data disposal when an organization no longer needs biometric information for the collection purpose.

Enforcement Mechanisms

BIPA permits a "person aggrieved" to bring an action in state or federal court and recover:

- For each negligent violation, the greater of:
  - liquidated damages of $1,000; or
  - actual damages.
- For each intentional violation, the greater of:
  - liquidated damages of $5,000; or
  - actual damages.
- Reasonable attorneys' fees and costs.
- Injunctive or other appropriate relief.

(740 ILCS 14/20.)

By contrast, only the attorneys general of Texas and Washington may bring actions to enforce their statutes.

Non-US Laws

Organizations with employees, customers, or business operations outside of the US must also comply with any data protection or sector-specific laws governing biometric data collection and use including, for example, the General Data Protection Regulation ((EU) 2016/679) (GDPR).

This Note focuses on US laws governing biometric data and other laws are outside the scope of this Note.

Cyber Insurance for Biometric Data Coverage

Cyber insurance provides much needed insurance coverage for organizations confronted with a potential or actual violation of biometric data laws.

However, comparing policies and selecting appropriate cyber coverage is rarely straightforward given the lack of policy standardization and the complex nature of data risks. For example, two forms may use the same terms, such as "security event" or "regulatory investigation," but they can define those terms differently, creating significant differences in the scope of coverage provided.

Coverage differences across policies can be substantial and may include variations in:

- The triggering of notice requirements.
- Scope of coverage, including for regulatory exposures.
- Aggregate policy limits and sub-limits.
- Self-insured retentions.
- Coverage periods, including retroactive coverage.

Cyber policies should cover biometric-data privacy claims in the absence of any exclusions or limiting language, but policyholders must check to ensure that their policies address certain issues including:

- Cyber policies typically cover claims arising from "privacy events" or "privacy and security wrongful acts" which may include the unlawful or unauthorized disclosure of confidential or private data. This language should cover biometric data law violations based on the unauthorized collection, storage, or other use of the data, including unauthorized transmission of that data to third parties.
- Some cyber policies may define "confidential" or "private" data in a way that may limit coverage for biometric data.
- Some cyber policies also limit or exclude coverage for claims arising under specific, enumerated statutes, such as biometric data laws.

To date, no published decisions address companies seeking coverage for biometric data violations under cyber policies. Many policyholders without cyber insurance have also sought coverage for biometric data-related losses in recent years under traditional, non-cyber policies with success. These types of claims are called "silent cyber" or "non-affirmative cyber claims" because the policies may not explicitly include or exclude cyber risk.

Commercial General Liability (CGL) Policies

General commercial liability policies (CGL) typically include coverage for "personal and advertising injury," in addition to coverage for bodily injury and property damage.

CGL policies typically define "personal and advertising injury" to include injury arising out of "oral or written publication of material that violates a person's right of privacy." Some CGL policies contain exclusions for Access or Disclosure of Confidential or Personal Information, which insurers argue bar coverage for biometric-data claims.

For more on exclusions under CGL policies that may apply to cyber-related claims, see Practice Note, Cyber Coverage Under Traditional Insurance Policies: General Commercial Liability Policies.

Meaning of "Publication" Disputes

CGL policies typically define personal and advertising injury as "oral or written publication, in any manner, of material that violates a person's right to privacy." Insurers frequently dispute coverage for BIPA lawsuits brought against the insured claiming that the underlying lawsuits do not specifically allege publication of material that violates a person's right of privacy.

In *West Bend Mutual Insurance Co. v. Krishna Schaumburg Tan, Inc.*, the Supreme Court of Illinois specifically rejected this argument and held that CGL policies cover BIPA claims. In *Krishna Schaumburg*, the insurer filed a declaratory judgment action seeking a determination that it did not owe its insured, a tanning salon, a duty to defend a class action lawsuit alleging BIPA violations arising from the disclosure of fingerprint information to a third-party vendor. The policies specifically defined "personal injury" and "advertising injury" as injury arising out of oral or written publication of material that violates a person's right of privacy. (2021 WL 2005464 (Ill. Sup. Ct. May 20, 2021).)

The insurer argued that a personal and advertising injury did not exist because "publication" requires communication of information to the public at large, not a single third party.

The Illinois Supreme Court rejected that argument and held that:

- The disclosure of the customer's fingerprint to a single vendor in alleged violation of BIPA constituted a publication under the common understanding and dictionary definition of the term.
- The allegations in the class action complaint that the policyholder tanning salon shared biometric information with a third party constituted a covered claim for "personal and advertising injury" within the purview of West Bend policies.

(*Krishna Schaumburg*, 2021 WL 2005464, at *7.)

Krishna Schaumburg may resolve pending complaints filed by insurers alleging similar arguments on the meaning of publication to bar BIPA coverage (see, for example, *Citizens Ins. Co. of Am. v. N.W. Pallet Servs., LLC,* No. 1:21-cv-02804, ¶¶ 38-40 (N.D. Ill. May 25, 2021) (Citizens Insurance filed a complaint disputing coverage because the employee complaint did not allege any "publication" and therefore does not allege "personal and advertising injury")).

Organizations seeking to rely on CGL coverage for biometric data violation claims must examine the language in their policies defining "publication" and understand potential arguments insurers may make to deny BIPA coverage.

Exclusions for Employment-Related Practices

CGL policies often contain personal and advertising injury exclusions for injuries arising out of employment-related practices, policies, acts, or omissions. Several insurers have disputed coverage based on this language for costs

to defend against employee lawsuits alleging biometric data violations.

For example, in *American Family Mutual Insurance Co., S.I. v. 1876 Clark LLC*, the insurer claimed that this exclusion barred defense coverage for a class action lawsuit alleging that the insured's fingerprint scanning to track its employees' time violated the BIPA (No. 1:21-cv-02991, at ¶ 267 (N.D. Ill. June 3, 2021); see also, for example, Compl. for Declaratory J., *Citizens Ins. Co. of Am. v. Nw. Pallet Servs.*, LLC, No. 1:21-cv-02804, ¶¶ 38-40 (N.D. Ill. May 25, 2021); Compl. for Declaratory J., *Old Republic Union Ins. Co. v. McDonald's USA, LLC*, No. 2021CH02445, ¶ 82 (Ill. Cir. Ct. May 19, 2021)).

These pending cases have not yet answered the question of whether an employment-related practices exclusion bars coverage for employees' BIPA claims. However, decisions outside of the BIPA context suggest that the exclusion may not apply because BIPA claims do not arise out of an employee relationship itself including hiring, firing, or job performance (see for example, *Peterborough Oil Co. v. Great Am. Ins. Co.*, 397 F. Supp. 2d 230, 238-39 (D. Mass. 2005) employment-related practices exclusion only applies to matters that "directly concern the employment relationship itself."); *Am. Econ. Ins. Co. v. Haley Mansion, Inc.*, 2013 WL 1760600, at *5 (Ill. App. Ct. Apr. 23, 2013) (holding that an employment-related practices exclusion did not apply to alleged defamatory remarks because they did not relate to a former employee's job performance)).

Statutory Exclusions

Some CGL policies contain exclusions barring coverage for personal and advertising injury claims arising directly or indirectly out of any action or omission that violates or is alleged to violate:

- The Telephone Consumer Protection Act.
- The Controlling the Assault of Non-Solicited Pornography and Marketing (CAN-SPAM) Act of 2003.
- Any statute, ordinance, or regulation, other than the TCPA or CAN-SPAM Act of 2003, that prohibits or limits the sending, transmitting, communicating, or distribution of material or information.

In *Krishna Schaumburg*, the insurer denied coverage arguing the policies' "other than" language in the violation of statutes exclusion barred coverage for the alleged BIPA disclosures. The court disagreed and found this exclusion only applies to statutes that govern certain methods of communication, such as emails, faxes, and phone calls and does not apply to statutes that "limit the sending or sharing of certain information," such as BIPA. (*Krishna Schaumburg*, 2021 WL 2005464, at 9.)

The *Krishna Schaumburg* ruling on the statutory exclusion language for BIPA coverage is likely to impact the current pending cases making similar arguments.

Access or Disclosure of Confidential or Personal Information Exclusion

Recent lawsuits filed by insurers disputing biometric data-related coverage concern language excluding personal and advertising injury coverage arising out of access to or disclosure of any person's or organization's confidential or personal information, including:

- Financial and credit card information.
- Health information.
- Any other type of nonpublic information.

(See, for example, *Citizens Ins. Co. of Am*, No. 1:21-cv-02804, at ¶ 53; *Am. Family Mut. Ins. Co., S.I. v. 1876 Clark LLC, et al.*, No. 1:21-cv-02991, at ¶ 267 (N.D. Ill. June 3, 2021); *Ins. Co. of Am. v. Wynndalco Enters., LLC*, No. 1:20-cv-03873 (N.D. Ill. Apr. 15, 2021); *Soc'y Ins. v. Cermak Produce* No. 11 Inc., No. 1:21-cv-01510 (N.D. Ill. Mar. 18, 2021); *State Auto. Mut. Ins. Co. v. Tony's Finer Foods Enters., Inc.*, No. 1:20-cv-06199 (N.D. Ill. Oct. 19, 2020).)

Insurers have argued that biometric data is confidential or personal information and the exclusion bars coverage for claims alleging biometric data disclosures. No courts have issued decisions on these cases to date, but the plain meaning of BIPA suggests this exclusion should not apply because BIPA states that:

- Biometrics differ from "other unique identifiers that are used to access finances or other sensitive information" because they are biologically unique to the individual (740 ILCS 14/5(c)).
- Biometric identifiers do not include information collected, used, or stored for healthcare treatment (740 ILCS 14/10).

Courts may hopefully produce one or more decision analyzing whether this exclusion applies to BIPA claims in the near future.

Employment Practices Liability Policies

Employment practices liability (EPL) policies are another type of insurance that can potentially cover biometric

data privacy claims. EPL policies cover businesses against claims by employees alleging company violations of their legal rights. These coverages may be written as stand-alone insurance policies or combined into a single policy with other insurance coverages (such as directors and officers coverage).

Disputes on Scope of EPL Coverage

Twin City Fire Insurance Co. v. Vonachen Services Inc. represents some of the potential coverage issues that may result when relying on EPL policies for biometric data claim coverage. Vonachen's policy provided coverage for the following commonly defined policy terms:

- "Employment practices wrongful act," defined as a breach of any oral, written, or implied employment contract including obligations arising from a personnel manual, employee handbook, or policy statement.
- "Employee data privacy wrongful act," defined as the failure to notify any employee or applicant for employment of "any actual or potential unauthorized access to or use of private employment information of any employee or applicant for employment" if any state or federal regulation or statute requires notice.
- "Private employment information," defined as any information regarding an employee or applicant collected by the insured to establish, maintain, or terminate an employment relationship.

(2020 WL 7073619 (C.D. Ill. Sept. 20, 2020).)

In its employee handbook, Vonachen represented that it intended to comply with all applicable laws and regulations. Vonachen sought coverage to defend against class action lawsuits alleging that it violated the BIPA when collecting employees' fingerprints for timekeeping purposes in reliance on the "employment practices wrongful act" and "employee data privacy wrongful act" language.

Twin City filed a declaratory judgment seeking a determination that it owed no insurance coverage to Vonachen related to the lawsuits because, among other things, the only claims asserted in the complaint concerned BIPA violations and not a breach of an employee handbook or contract(*Twin City*, 2020 WL 7073619).

The parties cross moved for summary judgment and those motions are currently pending before the court.

Breach of Contract Exclusions

Organizations seeking coverage under EPL policies may also face coverage arguments that the policy excludes coverage for costs arising from a breach of employee contracts.

In *Vonachen*, for example, Vonachen sought coverage based on the definition of an "employment practices wrongful act" which covered obligations arising from a personnel manual, employee handbook, or policy statement. Twin City argued against coverage because the EPL policy excluded claims "based upon, arising from, or in any way related to liability incurred for breach of any oral, written, or implied employment contract."

The court has not yet ruled on the scope of this provision.

Directors and Officers Liability Insurance

Directors and officers (D&O) liability insurance covers exposures faced by directors and officers and the company itself that arise from actual or alleged wrongful acts. However, the policy exclusions in these policies differ and can create ambiguities in coverage for biometric data claims.

The insurer in *Twin City Fire Insurance Co. v. Vonachen Services, Inc.* illustrates D&O insurers may dispute biometric data coverage costs. In that case, Twin City argued the following exclusions applied to avoid biometric data coverage:

- **Invasion of privacy exclusion**. The D&O coverage part of the policy provided that it did not cover losses related to any claim "based upon, arising from, or in any way related to any actual or alleged 'invasion of privacy.'" Twin City disputed coverage by arguing that the BIPA allegations in the underlying complaint relate to an actual or alleged invasion of privacy.
- **Insured versus insured exclusion**. The D&O coverage in *Vonachen* excluded claims brought or maintained by or on behalf of any "Insured" or "security holder of an Insured Entity." Twin City disputed coverage because employees qualify as Insureds and an employee brought the underlying BIPA claim.

(*Twin City*, 2020 WL 7073619.)

Vonachen's D&O coverage also contained an exclusion for employment-related wrongful acts which excluded losses related to any claim based on, arising from, or in any way related to any or actual employment-related wrongful act. Twin City did not raise this exclusion as ground for non-coverage, presumably because doing so may be an admission that the EPL coverage of the policy should have covered the underlying claim.

However, an insurer of a standalone D&O policy (without an accompanying EPL coverage) is likely to raise this exclusion as a ground for denying coverage in a lawsuit brought by employees alleging BIPA violations (see, for example, Compl. for Declaratory J., *Am. Family Mut. Ins. Co. v. McEssy Inv. Co.*, No. 1:20-cv-05591, at ¶ 13 (N.D. Ill. Sept. 21, 2020)).

Guidance for Organizations Needing Insurance for Biometric Data Claims

Organizations seeking insurance coverage for biometric data-related claims and costs must take the following measures:

- Assess the risks of facing a biometric violation or claim (see Assess Risks of Biometric Data Claims).
- Review current policies to evaluate potential disputes (see Review Existing Policies and Coverages).
- Understand the importance of the choice of law selection in policies (Understand Choice of Law Selection).

Assess Risks of Biometric Data Claims

Selecting effective biometric data coverage requires a business to consider the nature of biometric data claims it may face and seek insurance coverage that addresses those risks.

For example, organizations should understand the biometric data they collect and identify any laws applicable to that data. This should include data that the company discloses or outsources to third-party vendors. Organizations subject to the BIPA may also face additional liability from private lawsuits which they should consider when selecting coverage.

Organizations should collect information from multiple stakeholders to accurately identify and assess these risks, including:

- Information technology (IT) and information security.
- The privacy or compliance office.
- Human resources (HR).
- Business operations, including product or service development.
- Legal and risk.

This cross-disciplinary approach is necessary to assess the business's risk profile for biometric data claims and to determine the appropriate coverage needed.

Review Existing Policies and Coverages

Policyholders should review their existing policies to determine whether they may cover biometric data costs and identify potential exclusionary language that may bar coverage.

Disputes about insurance coverage frequently focus on a few words within a policy. Organizations should therefore ensure their policy language provides adequate protection by:

- Analyzing all potential biometric data claim scenarios against the policy language.
- Identifying all ambiguous language and provisions in each policy.
- Reviewing all definitions in each policy to ensure they are broad enough to cover biometric data claims.
- Ensuring that the organization understands and can comply with each policy's terms and conditions.
- Reviewing all exclusions to ensure that they do not prevent biometric data coverage.

If necessary, organizations should negotiate better coverage terms (or remove or revise potentially troublesome exclusions) at either policy issuance or renewal. Many companies use insurance brokers to help place their policies. Brokers do not practice law, but they can help identify what forms specific insurers have agreed to in the past.

Although insureds are often successful in seeking coverage for biometric data costs under traditional insurance policies, they may encounter insurer challenges to coverage based on the policy terms, conditions, and exclusions. However, in many cases, a standalone cyber policy may be the best solution to ensure broad coverage.

Policyholders should consult insurance attorneys to review their policies for potential gaps in coverage for biometric data privacy. Although this may be an extra expense on the front end, it is likely to save time and money if an insurer disputes coverage and litigation on the scope of the policy occurs on the back end.

Understand Choice of Law Selection

State law governs insurance disputes and the substantive laws vary significantly from state to state. A court's interpretation of insurance contract language under the applicable state's law can mean the difference between a coverage victory and loss. Organizations should work

with their counsel to examine the best forum and choice of law for litigating coverage disputes. If insurers try to add specific choice-of-law provisions, policyholders should also ensure they understand the ramifications of that choice.

Organizations reviewing polices to cover biometric data claims should also stay abreast of the ongoing litigated issues concerning biometric data coverage.