IS THAT COVERED?

Biometric Data Risk Sparks Insurance Market Reaction

What do Snap's $35 million settlement, TikTok's $92 million settlement, and Google's $100 million settlement all have in common?

These settlements were all reached in 2022 through class action lawsuits brought forth under the Illinois Biometric Information Privacy Act (BIPA). 2022 saw one BIPA class action lawsuit after another, and there are no signs that massive settlements and verdicts brought under this statute will slow down in 2023.

With the Illinois Supreme Court endorsing a five-year statute of limitations for BIPA claims in February 2023, and additional states enacting similar pieces of legislation, it's clear that the ubiquity of biometric privacy lawsuits is likely to persist in the years to come. Nearly 2,000 lawsuits have been filed since 2017 alleging violations of BIPA alone. And the insurance market is paying attention, with several carriers beginning to add BIPA exclusions to their policies.

It's clear that business leaders everywhere need to be aware of this complex and significant risk and take the necessary steps to ensure they remain compliant with evolving regulations in the space. Here's what you need to know about biometric data risk, how insurance fits into the picture, and what you can do about it.

WHAT IS BIOMETRIC DATA & HOW IS IT REGULATED?

Biometrics are unique, intrinsic physical and behavioral human characteristics that can be used to digitally identify a person to grant them access to devices, data, or systems. Fingerprints, facial patterns, eyes, and voice are just some examples of biometric identifiers.

Though there are no biometric data privacy regulations at the Federal level, a few states have enacted legislation to regulate private entities' handling and processing of biometric information. The oldest and most notable of these statutes is the Illinois Biometric Information Privacy Act.

Read an overview of biometric privacy laws here.

AHT INSURANCE
A BALDWIN RISK PARTNER

WHY IS THIS A RISK FOR ORGANIZATIONS?

Organizations that collect, handle, and store biometric identifiers of either employees or customers in any capacity need to be aware of the risks of doing so. **These risks include:**

- **Regulatory risk** – Failure to comply with biometric privacy laws makes your organization susceptible to fines from state government entities.
- **Litigation risk** – BIPA specifically contains a damages provision. This is what's opened the floodgates for class action lawsuits where companies found to be negligent have been forced to pay settlements that have regularly been millions to hundreds of millions of dollars.
- **Cyber risk** – Malicious actors have found ways to steal and use biometric data to then access protected virtual systems. Cyber breaches are very costly incidents to remediate.
- **Reputational risk** – When a password is compromised after a breach, affected individuals can easily change it. This isn't the case with one's fingerprints, iris pattern, voice, and facial structure, which is why the reputational fallout from failing to protect biometric identifiers can create even more liability.

HOW DOES INSURANCE FIT INTO THE PICTURE?

In the event of a biometric data privacy lawsuit, several policies may be at play depending on the nature of the claim and policy language. This is because claims may be brought forth by both employees and customers, and data-related claims could be seen as a cyber liability issue. Companies that face these claims might have a range of options for insurance coverage, but you should never assume that biometric liability is covered by your existing insurance portfolio.

- **Commercial General Liability (CGL)** – Because CGL policies cover such wide-ranging events, you might assume that a biometric privacy claim is covered. However, many CGL policies have exclusionary language that might bar this event from coverage.
- **Employment Practices Liability (EPLI)** – Depending on the wording of the policy, biometric privacy claims may or may not be covered. Some EPLI policies explicitly exclude invasion of privacy or sublimit claims related to employees' private information.
- **Directors and Officers (D&O)** – This type of claim might trigger D&O coverage, but many D&O policies exclude bodily injury, property damage, and invasion of privacy language which may preclude biometric data privacy claims from coverage.
- **Cyber Liability** – Depending on the nature of the claim, a cyber policy may or may not respond to a biometric data privacy lawsuit. If the claim occurs as part of a data breach, regulatory action, or private right of action claims, a cyber policy might kick in. However, a cyber policy wouldn't kick in as a response to shareholder litigation.

When we consider how biometric privacy lawsuits are continuing to pile up and how costly they can be for companies that are found to be negligent, it's not surprising that policyholders and carriers are grappling with how to address and cover this exposure. However, in many cases when carriers have tried to deny coverage for these claims, the courts have ruled in favor of policyholders. Because of the circumstances at hand, some carriers are now explicitly excluding biometric data privacy claims.

HOW CAN YOU PROTECT YOUR COMPANY FROM THIS EXPOSURE?

Fortunately, if your company collects biometric identifiers from employees and/or customers there are steps you can take to reduce the likelihood of a claim:

- **Understand the types of biometric data you collect** and how laws in various states apply to that data, including any information you share with third-party vendors.
- **Align relevant stakeholders within your company** so that all relevant parties are aware of the risk at hand and collaborate to minimize it with the appropriate policies, procedures, and safeguards. Relevant stakeholders may include the following departments: IT, compliance, the Board of Directors, HR, business operations, and legal.
- **Develop a biometric collection and retention policy** that clearly delineates which data is being collected, the reason for collecting this data, how you plan to safely store and share the data, the length of time you will store or share the data, and how you plan to dispose of the data.
- **Ensure that you include all information** regarding your biometric data policy within your employee handbook.
- **Create a biometric consent approval form** for both employees and customers. This should also include information regarding your collection and retention policy. Be sure you have signed consent forms from individuals before collecting their biometric data.
- **Understand insurance policy language and identify exclusionary language or sublimits** that could create coverage gaps in the event of a claim. Align your legal experts with your insurance broker so that you're covered from biometric privacy claims and can buy coverage endorsements if needed.

As the regulatory landscape regarding biometric data continues to evolve, you need to be aware of how these changes could impact your business and how your insurance coverage might respond. With some carriers moving to exclude biometric data privacy claims, it's important for you to work with an experienced broker who can negotiate on your behalf so that you're covered from this significant exposure.

Learn more about what you can do to address biometric data risk. Connect with one of our Cyber experts to help protect your organization from this complex liability.

AHT INSURANCE
A BALDWIN RISK PARTNER