Biometric Information Privacy Laws Could Have Major Consequences

The Illinois Biometric Information Privacy Act (BIPA) was the first state statute to restrict when and how entities can collect, purchase and obtain biometric identifiers (e.g., fingerprints, voiceprints and retinal scans). BIPA requires private entities to:

1. inform individuals that their biometric information is being collected or stored;
2. notify the individuals in writing of the specific purpose and length of time for which the biometric information is being collected, stored and used; and

3. receive written releases from the individuals to collect, store and use such biometric information.

Other states, including Texas and Washington, have since enacted biometric privacy statutes, but BIPA is unique because it provides individuals with a private right of action to assert claims against entities. To date, most BIPA-related lawsuits have arisen in the employment context — specifically where an employer replaces "punching a time-clock" with a time-card system dependent on collecting and storing employees' biometric identifiers.

However, in the recent case of **Rosenbach v. Six Flags Entertainment Corp.**, which addressed Six Flags' collection of biometric data from its season pass holders, the Illinois Supreme Court held that individuals have standing to sue for BIPA violations, even if they suffered no actual harm as a result of such violations. Because of Rosenbach, consumer lawsuits under BIPA are expected to increase dramatically.

Following Illinois' Lead

Other states are beginning to follow Illinois' example. Most notably, on January 11, 2019, Massachusetts State Senator Cynthia Creem introduced a consumer data privacy bill that, while broader in scope than BIPA, places similar restrictions on the collection and use of consumers' biometric information. The proposed law expressly provides consumers with a private right of action, regardless of whether the consumer can show any loss of property or money arising from the violation.

Although the proposed law is still in its legislative infancy and would not go into effect until 2023 if passed, it is inevitable that states will continue to enact more restrictive data privacy laws. The proliferation of more restrictive data privacy laws is of interest to all insurers for two reasons. The first is that insurers will be subject to these laws, just like every other entity that collects, stores or uses individuals' personal data. The second is that alleged violators of such laws are likely to seek coverage under their insurance policies.

Compliance with Data Privacy Laws by Insurers

Most state data privacy laws apply based on the consumer's state of residency and not on where the entity collecting the data is domiciled. For instance, a company headquartered in Rhode Island but with employees who reside in Massachusetts must comply with Massachusetts' data privacy laws with respect to its Massachusetts resident employees, even if those employees work at the company's Rhode Island office. Similarly, if the Rhode Island-headquartered company collects private information on Massachusetts consumers, it must comply with Massachusetts' data privacy laws with respect to those consumers.

Because many insurers operate at an interstate or sometimes national level, they may be particularly susceptible to unintentionally violating the privacy laws of the states in which their employees and customers reside. Rather than merely complying with state laws in the states where they maintain offices, they will need to

comply with a patchwork of different state laws governing the collection, storage and use of data from employees and customers living in different states. As more states provide consumers with private causes of action regardless of actual harm, engaging in interstate business operations will greatly increase such businesses' potential exposure.

Insurers may also be at heightened risk because of the highly sensitive personal data and health information collected as part of the underwriting process. Some insurers may even collect biometric data. Insurers that collect any kind of biometric data from their employees or customers should proactively consider the risks associated with collecting such information in light of BIPA and other similar statutes that are sure to follow (including the Massachusetts proposed law).

Compliance with Data Privacy Laws by Insureds

Unlike many other businesses, insurers are also exposed to potential liability through the activities of their customers. BIPA lawsuits are bringing to light new questions regarding the scope of coverage under existing insurance policies. As additional states pass biometric information privacy laws, disputes over the scope and amount of insurance coverage for such claims will inevitably increase.

Using BIPA as an example, violations by insureds could potentially lead to coverage exposure. For instance, an insured could claim that its improper use of biometric identifiers for time-tracking purposes should be covered by employers' employment practices liability insurance (EPLI) policies, and such liability would be significant. The penalty for BIPA violations is the higher of actual damages or $1,000 per negligent violation or $5,000 per intentional or reckless violation.

Thus, putting aside the question of whether each check-in and check-out constitutes a separate violation, an employer with 100 employees could easily face damages in excess of $100,000 for implementing a time-card system that improperly utilizes biometric data. Unless the industry takes affirmative action to clarify policy language, the courts will likely determine the scope of coverage.

It is less likely that typical commercial general liability (CGL) policies would cover BIPA violations, because approximately five years ago, most insurers began inserting exclusionary language to preclude coverage under CGL policies for data breach and cybersecurity liability and offering them as separate additional coverage. However, if an insurer's CGL exclusion language has not been updated, the earliest violations might still be covered by its CGL policies.

In the consumer context, a consumer may claim that bodily injury coverage contained in standard CGL policies should cover claims alleging infliction of emotional distress arising from the improper collection of biometric data. As with EPLI policies, questions related to coverage will likely be decided by the courts. Consequently, it is even more important for insurers to clearly define the exclusions from coverage in their policies.

Certain cybersecurity liability insurance policies might include definitions of "confidential information" or "personal information" that were drafted so generally or broadly that biometric data could be deemed included. In such cases, these policies could be interpreted to cover breaches of biometric privacy laws. There is also a stronger argument for coverage if the insured transmits such information to third parties (for instance, a data processor that assists with maintaining the insured's customer records) because such policies typically cover disclosures to third parties. Because cybersecurity liability insurance policies are relatively new and often vary from policy to policy, whether a given policy will apply to a particular scenario is likely to be a fact-intensive question.

Insurers should consider whether and how their cybersecurity liability insurance policies might be construed with respect to claims related to biometric data and modify their policy language as necessary.

Finally, there are also less common insurance policies (such as media liability insurance policies) that tend to be tailored to a particular customer's business and which may trigger coverage for violations of biometric information privacy laws. To the extent that insurers offer such customized or infrequently issued policies, they should evaluate the policy language to make sure that they are not bound to insure against risks for which the

policies were not intended.

Conclusion

Because biometric information privacy statutes are relatively new, there are still many unknowns regarding where, when and how they will be implemented and how they will impact the industry. It is clear, however, that such legislation will continue to gain traction, with unfavorable consequences for the unwary. Therefore, insurers would be wise to consider the risks associated with both their current data collection, retention and usage practices and the practices of their insureds. Policy language should also be reviewed in light of the additional coverage exposure posed by biometric information privacy laws.

Date Created
May 3, 2019