FINE PRINT

Insurance Considerations for Biometric Liability

by Cort T. Malone and Jade W. Sobh

Across the United States, state legislators are introducing and passing new biometric privacy laws that create varying degrees of liability exposure. These new laws should spur businesses to assess both their collection and use of biometric information and the insurance policies they would tap to cover any exposure to biometric liability.

At present, four states—Illinois, Texas, Virginia and Washington—have enacted biometric privacy laws that specifically require giving notice and obtaining consent before collecting biometric information, and many other states regulate the collection and handling of biometric data in more limited ways. Several states have pending legislation modeled to varying degrees on Illinois' pioneering Biometric Information Privacy Act (BIPA), which was enacted in 2008 and is the most stringent of the existing state biometric privacy laws. In the first quarter of 2022 alone, seven states introduced biometric privacy legislation sharing key features of BIPA. These bills may have varying impact depending on factors such as whether or not they create a private cause of action, the size of fines assessed per violation, and whether they allow for a notice period and opportunity to cure.

BIPA is currently the only enacted state law that creates a private right of action for individuals harmed by biometric privacy violations (New York City's law also creates a private right of action, but liability exposure is mitigated by a curing period). BIPA provides statutory damages up to $1,000 for each negligent violation and up to $5,000 for each intentional or reckless violation. Due in large part to the private right of action, which opens the door to broad-based class action suits, BIPA has resulted in some of the largest settlements of all the biometric identifiable information privacy laws, including a $100 million settlement by Google.

Last October, in the first trial to go to judgment for BIPA violations, a federal jury in Chicago awarded a $228 million verdict to the class action plaintiffs. In the case in question, *Rogers v. BNSF Railway Co.*, a truck driver alleged that BNSF Railway violated BIPA by scanning and retaining employees' fingerprints at its railyards without obtaining written informed permission, and without publishing a data retention or destruction schedule. After a five-day trial, jurors found that BNSF "reckless[ly] or intentional[ly]" violated BIPA 45,600 times, which matched an estimated number of truck drivers who had their fingerprints registered.

The insurance industry is likely to take note of this escalation in biometric liability exposure. While insurance companies faced with biometric liability claims have invoked general exclusions pertaining to disclosure of confidential information and data-related liability, many courts have held that such exclusions do not preclude coverage for BIPA violations. Accordingly, insurance companies are beginning to include more specific exclusions, which already appear in some general liability policies and employment practices liability insurance policies. In the wake of Rogers, these exclusions also may start to become more common in other policies, such as cyber and directors and officers policies.

The basis of the $228 million award also may impact BIPA claim settlement negotiations. Enterprising insurance companies may contend that *Rogers* increases the chances of a verdict for "reckless or intentional" violations, which insurance companies may argue constitutes potentially excluded "intentional" conduct. However,

RISK MANAGEMENT

Reprinted with permission from *Risk Management*.

www.rmmagazine.com

the jurors in Rogers did not decide whether BNSF's conduct was either reckless or intentional. Moreover, as insurance companies are aware, the question of whether a company knowingly violated the law often depends on the facts of each case, making broad generalizations from *Rogers* inapplicable.

While recently enacted and pending state biometric privacy laws vary considerably, liability exposures created by BIPA in Illinois are spreading to other states. Under some new and proposed laws, companies can be charged fines without intentionally violating the biometric privacy requirements, and some states do not allow for a period to cure, making liability almost certain for companies that do not take the necessary precautions. As noted above, the private right of action likely will spread to states other than Illinois.

Faced with the increase in biometric liability exposure, companies must take steps now to confirm that their insurance policies provide coverage for these types of statutory damages—regardless of whether a company currently utilizes or stores any biometric information. For existing insurance policies, businesses should work with brokers and coverage counsel to review all potentially responsive policies—including CGL, EPL, cyber and even D&O coverage—in light of both the relevant state privacy laws and the existing case law that mostly supports coverage under standard form CGL and EPL policies. A particularly important step is reviewing these policies for the most common exclusions that insurance companies have attempted to rely upon to deny coverage, as well as understanding how state court decisions have interpreted such exclusions. Even if existing policies contain terms favoring coverage under current biometric privacy law, companies must be extremely wary of insurance industry efforts to limit their exposure in new or renewal policies via BIPA-specific exclusions or sublimits for violation of biometric privacy statutes.

In addition to endeavoring to protect insurance rights, businesses also must remain vigilant and consult professionals to assess their potential liability under state privacy laws, including every state in which the company either sells products or provides services. R

Cort T. Malone is a shareholder in the New York and Stamford offices of Anderson Kill and practices in the insurance recovery and the corporate and commercial litigation departments. **Jade W. Sobh** is an attorney in Anderson Kill's New York office who practices in the insurance recovery and white collar defense departments.