Brown & Brown

PROPERTY & CASUALTY

Biometric Privacy

Risks, Trends and Mitigation

By Miles Crawford and Britt Eilhardt

You can now buy a cup of coffee simply by scanning the palm of your hand. Fingerprints secure our bank accounts. Facial recognition saves us time at the airport. These conveniences all employ forms of biometric technology and promise to streamline our day-to-day tasks. Yet, for many Americans, biometric technology is among the most significant areas of concern when asked about data privacy.

The potential for harm primarily lies in the fundamental nature of biometric identifiers. Unlike passwords or tokens, biometric identifiers are unchangeable and cannot be reissued. This means that compromising biometric information could have irreparable, lifelong consequences. Correspondingly, public concern has led to specific biometric privacy regulations that reach farther to enforce safeguards than general data privacy laws. In many cases, the penalties for misuse or mishandling of biometric information are severe. With courts, state and federal entities pushing the limits of existing biometric privacy regulations, it is crucial for businesses to remain updated on these matters and the changing landscape of compliance risks.

BIPA: The U.S. Pacesetter Still in Flux

In 2008, the Illinois state legislature passed the Biometric Information Privacy Act (BIPA), which established important standards for collecting and using biometric information. BIPA sought to address gaps in earlier data privacy regulations by specifically targeting the collection, use and storage of biometric information. One of the most significant, original features of BIPA is its provision for a private right of action. This means that individuals can file lawsuits against companies for violations of the law, even without proving actual harm. Additionally, BIPA imposes significant penalties for violations: up to $1,000 per violation or $5,000 if the activity is intentional or reckless. This has led to a spike in high-profile lawsuits against companies for allegedly violating BIPA's requirements, resulting in increased risks for businesses that handle biometric data.

Now, 15 years later, the implications of BIPA are still evolving. A recent uptick in BIPA -related cases has expanded the law's applicability and penalties. Additionally, while BIPA is an Illinois state law, its impact has extended beyond state borders. Companies operating in other states, and even internationally, have reassessed their biometric data handling practices, as data transfer across state and international borders is difficult to monitor and control. As a result, non-Illinois-based companies are implementing measures to align with BIPA's standards, to help avoid legal risks and maintain consumer trust.

Present Status of U.S. Biometric Privacy Regulation

Before 2018, only three U.S. states — Illinois, Texas and Washington — had privacy laws that specifically addressed biometric information. However, the number of states with such laws has grown dramatically since 2018. The pandemic-driven impetus for remote work and contactless technology drove a subsequent public interest in data privacy, translating into legislative action. In the first quarter of 2022, no fewer than seven states – California, Kentucky, Maine, Maryland, Massachusetts, Missouri and New York – introduced new biometric privacy regulations. Although there are variations in the language and force of each state's law, the general trend is for states to approach or match Illinois' BIPA standards.

Trends and the Potential for Future Regulation

The pandemic-induced bump in data privacy legislation will likely continue to produce new legislation at the state and federal levels. Although many new biometrics statutes pass state legislatures, these measures generally conform with the restrictions and provisions previously established by other states. Many states have expanded existing data privacy regulations to include specific provisions for biometric data rather than enacting standalone laws.

Legislators have demonstrated some interest in creating new regulations to address biometric privacy and security concerns at the federal level, but more conclusive legislative efforts are needed. The Federal Trade Commission announced in May 2023 that if entities employ biometric technologies in such a way that causes harm to consumers or uses deceptive or unfair practices, then those entities may be found in violation of the Federal Trade Commission Act of 1914. The agency has asserted that companies using these technologies are responsible for assessing foreseeable harms to consumers, promptly addressing known risks, determining if data collection is surreptitious, providing appropriate privacy training for employees and contractors, and holding third parties to the same standard.

Outside the U.S., the EU law (GDPR) classifies biometric data as a special category of personal data. The law may be stricter than in the U.S., but it is without a private right of action. GDPR allows companies to process biometric data only if it falls within one of the lawful reasons: processing with the explicit consent of the data subject or when processing is necessary for reasons of substantial public interest.

Insurance Implications

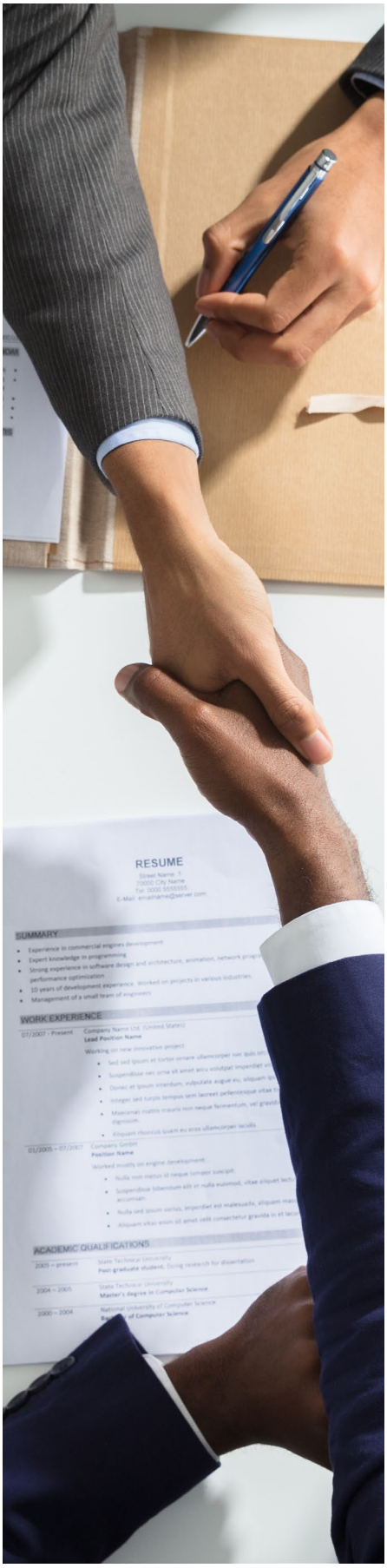
Cyber insurers have been focusing on collecting and storing biometric data risks. They are not only seeking more information from insureds, but they are reviewing insurance policies to understand potential coverage. Buyers of insurance should be doing the same. Cyber insurance policies can limit coverage to breach events and might not extend to non-compliance with statutes. Carriers have recently started adding specific BIPA or biometric exclusions to their policies, with some targeting specific industries or services and others excluding BIPA across the board.

Depending upon what constituency is being impacted by noncompliance with biometric legislation, D&O or EPL policies might be implicated. Some policies incorporate “invasion of privacy” exclusions, which could remove coverage under those programs. A review of the forms is recommended if a company is looking for protection under those programs.

Cyber insurance will likely be the coverage that most companies pursue to cover biometric liability. In seeking cyber insurance, insureds should ensure that coverage applies to all forms of records, that coverage is not limited to data breaches, and that the policy extends explicitly to privacy regulatory fines and penalties in the most favorable jurisdiction for coverage. To get favorable results, insureds should be ready to provide their brokers with a sound understanding of how they use biometric data, as well as the processes and controls used. They should also request a policy review from their broker to confirm they have the best the market can provide.

BIPA Guidance for Fines

- Intentional or reckless violations up to $5,000 each
- Negligent violations up to $1,000 each
- The settlements and verdicts can be significant - well over $100 million
- Courts recognize vicarious liability possibilities where a company directs the collection of biometric data



How Brown & Brown Can Help

Connect with our Brown & Brown team to learn about our knowledge in your industry, how we build our risk mitigation strategies and how we can aid your business in building a cost-saving program.

Brown & Brown

Find Your Solution at BBrown.com