Brown & Brown

PROPERTY & CASUALTY

# Biometric Privacy

## Recent BIPA Case Developments

By Miles Crawford and Britt Eilhardt

In our first article "Biometric Privacy, Risks, Trends and Mitigation", we discussed current biometric privacy regulation, trends and potential future regulation and the implications for insurance. Read more here: https://www.bbrown.com/insight/biometric-privacy-risks-trends-and-mitigation/

Many organizations are using biometric data, such as fingerprints and retinal scans, as a convenient way to improve security. From touchpads that unlock devices to scanners providing access to places of business, biometric data is a fast, easy and secure way to authenticate individuals and unlock access. The potential for harm lies in the fundamental nature of biometric identifiers. Unlike passwords or tokens, biometric identifiers are unchangeable and cannot be reissued. 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.

The precedent in the biometrics space is the Illinois 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 without proving actual harm. 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. Recent decisions on the interpretation of the law have increased exposure for companies utilizing biometric technology.

## Notable Case Law Developments

### Renderos v. Clearview AI – BIPA-Like Results Without BIPA

In November 2022, the Alameda, California, County Superior Court decided in Renderos v. Clearview AI, that existing privacy and unfair competition laws applied to biometric privacy violations, even without specific biometric privacy legislation. The case centered on Clearview AI's alleged scraping of facial data from public platforms and subsequent commercialization through facial recognition databases. The case encompassed claims related to misappropriation of likeness, invasion of privacy and unfair competition. The court found that common law privacy rights, the California constitution and the expansive California Unfair Competition Law offered grounds for private right to action akin to those under BIPA.

### Tims v. Black Horse Carriers, Inc. – Statute of Limitations

On February 2, 2023, the Illinois Supreme Court issued its decision on Tims v. Black Horse Carriers, Inc., providing greater clarity on the applicable statute of limitations. Previously, there was debate about whether a one-year or five-year statute of limitations applied to BIPA claims. The court's ruling established that all violations of BIPA would be subject to a uniform five-year statute of limitations, overturning a previous appellate court decision that had introduced differentiation between various violation types. In the Tims case, the plaintiff alleged multiple infringements of BIPA by their former employer, including the failure to establish a written biometric data retention policy, lack of informed consent and disregard for disclosure prohibitions. The Illinois Supreme Court's analysis emphasized the need for clarity and consistency for litigants and concluded that the five-year limitation should apply consistently to all BIPA violations. This decision amplifies potential liability for businesses lacking awareness of BIPA's provisions and underscores the importance of adopting preemptive measures for adherence to the law.

### Cothron v. White Castle System, Inc. – How Privacy Violations Are Quantified

On February 17, 2023, the Illinois Supreme Court ruled that every instance of scanning or transmitting a person's biometric identifiers constitutes a separate violation of BIPA. In the case of Cothron v. White Castle System, Inc., the plaintiff, an employee at White Castle, alleged that the company had repeatedly required her to scan her fingerprint without proper consent. With a 4-3 majority, the court agreed that each scan was a distinct violation. This decision has significant implications for damages, as BIPA awards $1,000 for each negligent violation and $5,000 for willful violations. With each scan considered a separate violation, potential damages could reach astronomical levels. For instance, White Castle estimated that damages for a 9,000-person class could amount to $17 billion. The court noted that the legislature should address these potential business-threatening penalties, but also acknowledged the courts' discretion in avoiding excessive damages that could financially destroy a business. Entities using biometric identifiers in Illinois should assess their compliance with BIPA's requirements.

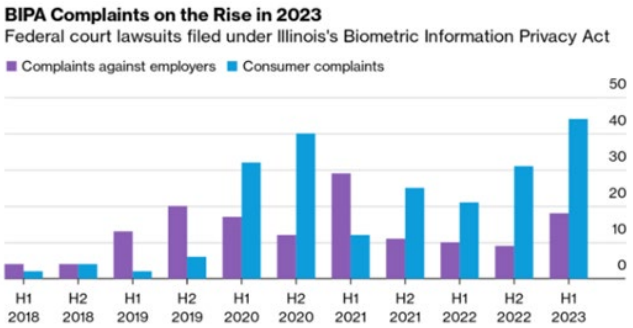
## Best Practice Recommendations

Risk mitigation in the era of biometric data is more critical than ever. Organizations that collect, or are considering collecting, biometric information on employees, customers or others should implement internal controls and human resources procedures. If a company retains vendors, it should have strict controls and take legal responsibility for any breach or non-compliance. Other steps companies should consider as a baseline for reducing risk include:

- Maintaining a public privacy policy with specific reference to biometric information
- Permanently destroying biometric information promptly if not required
- Providing notice to individuals before the collection of biometric information
- Seeking consent for any biometric information before its collection
- Maintaining security measures to safeguard biometric information at the highest levels
- Strictly prohibiting sales and any other form of profit from biometric information
- Maintaining policies for the transfer of biometric information to any third- party

Cyber insurers have been focusing on collecting and storing biometric data risks. Insureds should be ready to share with their brokers how they use biometric data and the processes and controls they have in place. This information will be critical to maintain coverage for fines and penalties in cyber programs for biometric data. As carriers look to add specific BIPA or biometric exclusions to their cyber and other policies, preparing for questions during the submission process will effectively maintain the broadest terms.

## Increase of Cases




Source: Bloomberg Law federal court dockets.

## Large settlements

| | | |
|---|---|---|
| **Facebook** | 2021 | $650M |
| **BNSF** | 2022 | $228M |
| **ID Verifier** | 2022 | $28.5M |
| **McDonalds** | 2022 | $50M |
| **Compass** | 2021 | $6M |

# 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**