Fingerprint Biometrics: Minimizing Risk in the Face of Increasing Liability

David J. Oberly

Just a few years ago, the thought of employees being able to "punch in" at work using their fingerprint seemed like pure science fiction. Today, fingerprint-based biometrics is widely used as a go-to method for organizational timekeeping.

At the same time, however, the use of biometric fingerprint readers have become the primary target for complex class action litigation under the Illinois Biometric Information Privacy Act ("BIPA"). To further complicate matters, various states and municipalities are enacting new, stringent laws modeled off BIPA to regulate the commercial use of fingerprint biometrics.

It is thus imperative that all companies using fingerprint biometrics take actionable steps to leverage this valuable form of biometric data in an effective fashion maintains compliance with the law and minimizes liability exposure.

Overview of Biometric Fingerprint Technology

Biometric fingerprint technology involves the process of using "biometrics" (*i.e.*, individual physical characteristics) to scan a person's finger and identify their finger "geometry" by measuring its length, width, thickness, and surface area. These measurements are then converted into a mathematical algorithm referred to as a "digital template" or "fingerprint template" and stored in a database.

Fingerprint biometric technology has become increasingly popular; it is now heavily relied upon in a range of different commercial contexts due to its ability to enhance the efficiency, effectiveness, and security of business operations.

But while fingerprint biometrics have produced a myriad of benefits, its use also carries significant privacy risks. Unlike other forms of personally-identifiable information, once compromised, fingerprint biometrics and other forms of biometric data lose their ability to be used as a secure identifying feature.

The Increasingly Complex Web of Biometric Privacy Regulation & Corresponding Liability Risk

To combat the risk posed by fingerprint biometrics and other forms of biometric data, several states have enacted laws that directly regulate the collection and use of fingerprint biometric data by business entities.

Illinois' BIPA is considered the most stringent state law. Under BIPA, a private entity cannot collect or store fingerprint template data without first providing notice, obtaining written consent, and making certain disclosures. BIPA also contains a private right of action provision that permits the recovery of statutory damages between $1,000 and $5,000.

Beyond Illinois, Texas and Washington have also enacted biometric privacy laws covering fingerprint biometric technology, which impose similar requirements related to notice, consent, and mandatory security measures.

This new wave of biometric privacy laws has created substantial liability. This risk arises primarily because of the statutory damages made available under BIPA, which the Illinois Supreme Court made much easier to recover due to a 2019 ruling that plaintiffs can pursue BIPA claims even where no actual harm or damage is sustained. As just one example of the tremendous liability posed by BIPA, in mid-2020 Facebook settled a major BIPA class lawsuit for a staggering $650 *million*—but only after the judge rejected Facebook's initial $550 million offer. Moving forward, companies utilizing fingerprint biometric data in connection with their business operations will continue to see a flurry of BIPA class action filings.

In addition, many states and cities are finding other ways to regulate the collection and use of fingerprint biometric data. One primary way states have done so is through broader consumer privacy laws, many of which include fingerprint data (and other forms of biometric data) within their definitions of covered "personal information."

State legislators have also amended their data breach notification laws to add fingerprint biometric data to the types of "personal information" which, if compromised, triggers breach notification obligations by impacted entities.

Combined, it is clear the risk of potential legal liability—with corresponding sky-high damage awards—will increase exponentially in the immediate future for those companies that utilize fingerprint biometrics in the course of their business operations.

Fortunately, there are several best practices companies can implement to minimize the risk of becoming embroiled in high-stakes class action litigation stemming from the use of fingerprint biometrics or other biometric data.

Privacy Policy

As a starting point, companies should ensure they are being transparent with their fingerprint biometric data activities by implementing a detailed fingerprint biometrics-specific privacy policy.

Privacy policies should encompass the following issues: (1) clear notice that fingerprint template data is being collected and/or stored; (2) the current and reasonably foreseeable purposes for which the company utilizes fingerprint template data; (3) how fingerprint template data will be used; (4) a description of the protective measures used to safeguard fingerprint template data; and (5) the company's fingerprint template data retention and destruction policies and practices.

These privacy policies should be made publicly-available, which, at a minimum, should entail inclusion in the entity's broader online privacy policy. Companies should also update their policies whenever any material modifications are made to their fingerprint template data management practices.

Notice

Second, to further support transparency, companies should provide conspicuous, advance notice of the use of biometric fingerprint technology before any fingerprint template data is captured, used, or stored. In so doing, companies should offer consumers meaningful notice regarding how fingerprint digital templates are created and how such data will be used, shared, and stored by the company. Where appropriate, or required by law, contextual and just-in-time notices may be necessary.

Written Release

Third, companies must obtain signed, written consent—in the form of a written release—from consumers or employees authorizing the company to collect, use, and store their fingerprint template data prior to the time any such data is captured or used for any purpose.

In signing the written consent, the individual should acknowledge he or she has read the company's fingerprint biometrics privacy policy, as well as the more specific, written notice provided regarding the company's collection and use of fingerprint template data. This consent should also make clear the individual consents to those policies and guidelines, as well as to the capture and use of their fingerprint template data, including the company's ability to share such data with any service providers or third-party vendors for business purposes.

Data Security

Fourth, companies must ensure they implement effective data security safeguards to protect all data captured, used, and stored through fingerprint biometric technology from improper disclosure, access, or acquisition. Companies should ensure they safeguard fingerprint template data: (1) using the reasonable standard of care applicable to their given industry; and (2) in a manner that is the same or more protective than that in which the company stores, transmits, and protects other forms of sensitive personal information.

Vendor Management

Finally, as most fingerprint biometric systems require the use of third-party vendors to supply the technology to process fingerprint biometrics, companies must also effectively manage risk and minimize liability in connection with vendors and other service providers.

First, prior to entering into an agreement with any vendor that will have access to biometric fingerprint data, companies must complete the necessary due diligence and vetting of all potential vendors to ensure their security measures are sufficiently robust.

In addition, companies should review and update their contracts with current vendors to take into consideration the principal issues raised by biometric data laws, including the addition of provisions mandating that vendors employ reasonable safety controls to properly protect fingerprint template data, delete such data when required (or requested by the company), and provide prompt notice in the event of a data breach.

Conclusion

Fingerprint biometrics has provided dramatic enhancements in the efficiency and effectiveness of company operations across a wide range of industries. At the same time, however, the emergence of this technology has also brought with it significant bet-the-company class action litigation exposure. Moving forward, this liability exposure will only increase as additional jurisdictions enact their own biometric privacy statutes.

Consequently, companies utilizing fingerprint biometrics—especially those located in jurisdictions where no biometric data laws currently exist—should take proactive measures to build out flexible, adaptable

biometric privacy compliance programs to ensure continued compliance with the ever-changing biometric privacy landscape. By doing so, companies can ensure they maintain legal compliance to mitigate potential risk. Including experienced counsel in this process remains an important first step that can pay significant dividends.

David J. Oberly is an attorney in the Cincinnati office of Blank Rome LLP and is a member of the firm's Biometric Privacy, Privacy Class Action Defense, and Cybersecurity & Data Privacy groups. David's practice encompasses both defending clients in high-stakes, high-exposure biometric privacy, privacy, and data breach class action litigation, as well as counseling and advising clients on a wide range of biometric privacy, privacy, and data protection/cybersecurity matters. He can be reached at doberly@blankrome.com.