Bloomberg Law

Professional Perspective

Protecting Biometric Data Privacy

Wynter Deagle, Molly DiRago, Anne-Marie Dao, and Yarazel Mejorado, Troutman Sanders LLP

Protecting Biometric Data Privacy

Contributed by Wynter Deagle, Molly DiRago, Anne-Marie Dao, and Yarazel Mejorado, Troutman Sanders LLP

Illinois passed its Biometric Information Privacy Act, 740 Ill. Comp. Stat. 14, in 2008, making Illinois the front runner in regulating and governing the collection and storage of biometric data. In the decade since, privacy advocates have hailed the law as the nation's strongest form of protection in the commercial use of such data, and several states have similarly enacted laws to address biometric privacy protection. BIPA has survived ongoing efforts by the tech industry to weaken it. In turn, it has resulted in a plethora of class action suits against companies across the U.S. that are not in compliance with BIPA. Other states could soon follow.

Given that the buying and selling of consumer data has become a multi-billion-dollar industry, businesses need to understand the risks posed by these regulations and consider taking steps now to mitigate those risks. This article reviews the Illinois law and best practices for minimizing exposure.

Collection and Use of Biometric Data

"Biometric data" measures a person's physical characteristics in order to verify one's identity or to authenticate a given user. It is generally separated into physiological biometrics, such as DNA, face shape, retinal scans, and fingerprints, and behavioral biometrics, such as an individual's thought patterns, specific movements, or the unique way they complete a security-authentication puzzle.

Biometric data must be unique, permanent, and measurable. Once biometric data is collected, it is compared and matched to information in a database. For example, every time someone unlocks a smartphone screen with facial recognition, asks Siri or Google Assistant for a weather update, or logs in to his or her online bank account using a fingerprint, he or she is using biometrics.

Illinois on the Forefront

Among other things, BIPA requires any private entity in possession of biometric information to develop a written policy, inform the owner of the biometric information in writing about the purpose for collecting the information and the length of time it will be stored, and obtain written consent for the collection, storage, and use of the data.

A critical component of BIPA is its private right of action, which allows "any person aggrieved by a violation" of the act to sue for steep liquidated damages: $1,000 for each negligent violation, $5,000 for each intentional or reckless violation, attorneys' fees and costs, and injunctive or other relief. 740 Ill. Comp. Stat. 14/20. To date, this private right of action has spawned hundreds of class actions.

No Injury Needed in State Court

Perhaps creating a perfect storm, in 2019, the Illinois Supreme Court held in *Rosenbach v. Six Flags Entertainment Corp.*, No. 123186, 2019 BL 24272 (Ill. Jan. 25, 2019), that a "violation, in itself, is sufficient to support the individual's or customer's statutory cause of action." In other words, an individual is "aggrieved" within the meaning of the Act by a mere technical violation—regardless of whether there is actual injury (such as a monetary loss).

The *Rosenbach* decision opened the floodgates to BIPA class actions, which have skyrocketed. More BIPA class actions were filed post-*Rosenbach* than the total amount filed in the 10 years prior. In the wake of *Rosenbach*, a new wave of costly BIPA class action lawsuits have flooded courts.

Article III Standing Unresolved

Whether a mere statutory violation is sufficient for Article III standing in federal courts, however, is a different question. Before *Rosenbach*, courts generally held that where an individual undoubtedly knew his or her biometric data was being collected, such as in *Santana v. Take-Two Interactive Software*, 2017 BL 416892 (2d Cir. Nov. 21, 2017), or *McCollough v. Smarte Carte, Inc.*, 2016 BL 248588 (N.D. Ill. Aug. 1, 2016), a statutory violation of BIPA, without more, was not a "concrete harm" that would confer Article III standing. The Ninth Circuit, however, held otherwise in *Patel v. Facebook, Inc.*, 932 F.3d 1264 (9th Cir. 2019). The *Patel* court reasoned that the Illinois legislature intended to give Illinois residents control over their

biometric information and therefore the collection and retention of the information in violation of BIPA was a concrete harm sufficient for Article III standing.

The Seventh Circuit will weigh in on this question in *Bryant v. Compass Group USA, Inc.*, Case No. 20-1443. On March 23, 2020, defendant Compass Group, which operates vending machines that utilize fingerprint scanning in order to purchase items, filed an appeal with the Seventh Circuit, asking whether mere loss of the right to control one's biometric information is sufficient to establish Article III standing. In a twist of typical litigation roles, in *Bryant*, defendant-appellant argued that federal courts should defer to Illinois state courts and find Article III standing is satisfied by statutory violations. Presumably this is because Compass Group (like many defendants) would prefer to litigate in federal court.

Whether or not *Bryant* follows *Rosenbach's* lead, *Rosenbach* has made it easier than ever for plaintiffs to file—and sustain—class actions against companies with a threat of millions of dollars in damages.

Universal Orlando Resort

For example, in May 2019, an Illinois resident filed a purported class action against the owner of Universal Orlando Resort claiming he was not informed that Universal Orlando would require him to scan his fingerprints as a condition of entry when he purchased a non-refundable admission ticket and, as a result, Universal Orlando failed to obtain informed consent for the collection and storage of his biometric information in violation of BIPA. His suit, on behalf of himself and purportedly all other Illinois citizens whose fingerprints were collected by Universal Orlando within the statute of limitations period, was potentially worth millions. *Jack Yozze v. Universal Parks & Resorts*, No. 2019-CH-06366 (Ill. Cir. Ct. filed May 23, 2019). The case was settled/voluntarily dismissed in Aug. 2019.

Google

Similarly, Google was sued in Feb. 2020 by an Illinois resident who alleges that "Unbeknownst to the average consumer, and in direct violation of §15(b)(1) of BIPA, Google's proprietary facial recognition technology scans each and every photo uploaded to the cloud-based Google Photos for faces, extracts geometric data relating to the unique points and contours (i.e., biometric identifiers) of each face, and then uses that data to create and store a template of each face—all without ever informing anyone of this practice." *Molander v. Google LLC*, No. 5:20-cv-00918-EJD (N.D. Cal. filed Feb. 6, 2020).

Facebook

Due to the high potential statutory damages, resolution of BIPA class actions may prove quite costly. In Jan. 2020, Facebook agreed to settle a BIPA class action concerning the collection of facial biometrics for $550 million. *In re Facebook Biometric Info. Privacy Litig.*, No. 15-cv-03747 (N.D. Cal.). Importantly, however, the judge overseeing Facebook's proposed $550 million settlement has expressed reservations over the amount and requested details about individual payouts, as well as more information on why the amounts are likely to be less than the minimum statutory amounts given the "clear mandate from the Illinois legislature that these violations had a price tag." Whether it is approved or rejected as an insufficient amount, the Facebook settlement will likely trigger a new wave of extremely costly BIPA class lawsuits that will flood courts.

Notably, these class actions are not just filed against Illinois private entities. Rather, because BIPA applies to Illinois citizens whose biometric data is collected outside of Illinois, the law implicates any company that collects the biometric data of an Illinois resident, including those that do not conduct any business in Illinois.

Best Practices for Minimizing Exposure

While currently only BIPA allows for a private right of action, other states including New York and Florida have introduced (but not enacted) laws similar to the Illinois law. Given the uptick in BIPA class action litigation and the rapidly evolving regulatory landscape, businesses that collect, store, or use biometric data—regardless of the state in which the business is located—should take proactive measures to comply with existing regulations and mitigate litigation risks.

Implement a Biometric Data Policy

A mandatory first step is to create and implement a comprehensive, written policy regarding the company's collection, use, storage, and safeguarding of biometric data. At a minimum, the policy should address the company's procedure for giving notice, the length of time and purpose for which biometric information will be stored, which third parties will be

given access to the information (if any), and how to obtain written consent when collecting, utilizing, and disclosing biometric information. In addition, the policy (including the retention schedule) must be made publicly available, such as by including it in the business's online privacy policy.

Implement Data Security Measures

Companies should also implement safeguards to protect biometric data from improper access or acquisition. These security measures must be reasonable in light of the industry and should be documented in a written information security program. At a minimum, it should detail the biometrics-specific security controls incorporated into its security program and how those controls are appropriate and tailored to the nature of the specific types of biometric data collected, used, transmitted, and stored by the entity.

Written Notice and Written Consent

Businesses should ensure they provide individualized, written notice before collecting, using or storing any biometric data. At a minimum, the notice should disclose in straightforward and easily understood language:

- That biometric data is being collected and stored
- The specific purpose for which the data is being collected and will be used
- The length of time the data will be stored and used
- The retention schedule and procedure for permanently disposing of biometric data
- The data security safeguards in place for biometric data
- If appropriate, that biometric data will be shared with service providers or third parties

It is equally imperative that, before any biometric data is collected, companies obtain signed, written consent acknowledging that the individual has reviewed the company's biometric data policy and written notice, and authorized the company to collect, use, and store the individual's biometric data.

Review Vendor Contracts

Contracts with third parties that receive biometric data should be reviewed and updated to require third parties to protect the biometric information transmitted to them and ensure they are utilizing biometric privacy best practices. These contracts should also include the right for the company to ask for information from the vendor about the security of the information, as well as a right to be notified in the event of a data security breach. Finally, a key provision in these contracts is the indemnification clause, which should provide the company with indemnity for litigation or regulatory action triggered by a vendor's data breach or violation of any privacy laws.