As Biometric Privacy Laws Grow, Cos. Must Up Transparency

By **Joseph Wylie, Katherine Staba and Kelsi Robinson** (July 10, 2023)

Joseph Wylie

Katherine Staba

Kelsi Robinson

Companies have increasingly leveraged the use of data derived from individuals' physical attributes — biometric data — such as fingerprints used for employee time clocks, voiceprints used to identify customers using customer service phone numbers and facial recognition to identify individuals in social media posts.

In response, many U.S. jurisdictions — starting with Illinois in 2008 — have enacted, or are considering enacting, statutes that regulate the collection, storage and usage of biometric data. These laws impose compliance standards, and provide both public and private enforcement mechanisms that pose considerable risks to companies collecting this regulated data.

While the landscape of states with a private right of action has been limited to Illinois for over a decade, the space is poised to rapidly evolve.

As more states begin to introduce biometric privacy legislation, it becomes imperative for businesses collecting biometric data to proactively address prior notice, disclosure, collection and deletion directives.

The First of Many: A Closer Look Into Illinois BIPA

The first state to enact a law specifically tailored to address biometric data, Illinois, has one of the toughest and most protective laws relating to biometric data protection in the country.

Over a thousand lawsuits have been filed alleging Biometric Information Privacy Act violations in the past 10 years,[1] which have resulted in multiple multimillion-dollar settlements.[2]

Under BIPA, "biometric information" is defined as "any information, regardless of how it is captured, converted, stored, or shared, based on an individual's biometric identifier used to identify an individual."[3]

Biometric identifiers include, for example, retina or iris scans, fingerprints, voiceprints, or any scan relating to the hand or face geometry — biometric information and identifiers are collectively referred to as biometric data.[4] Under BIPA, a company collecting biometric data must:

- Develop a publicly available written policy that establishes, notably, a retention schedule that provides for permanent destruction of biometric data no later than the earlier of three years from the individual's last interaction with the company or the satisfaction of the purpose for which the data was collected;

- Give prior notice to, and obtain written consent from, the individual whose biometric data is collected;

- Refrain from selling or otherwise profiting from an individual's biometric data;

- Refrain from disclosing or otherwise disseminating an individual's biometric data, unless the individual consents to such disclosure,[5] or the law requires it; and

- Store, transmit and protect all biometric data using a reasonable standard of care within the company's industry, and in a manner that is "the same as or more protective than" the manner in which the company stores, transmits, and protects other confidential information.[6]

BIPA allows a private individual to sue for any violation of the act where the individual is aggrieved by such a violation.[7]

The individual may recover $1,000 in liquidated damages per violation, which may be increased to $5,000 for intentional or reckless violations. However, the Illinois Supreme Court stated in Cothron v. White Castle System Inc. in February that trial courts have broad discretion to fashion appropriate relief — without providing guidance as to how that discretion should be exercised.[8]

Additionally, BIPA allows an award of attorney fees and costs for the prevailing party.

BIPA has led to an explosion of class action litigation, including one case — Richard Rogers v. BNSF Railway Co. in the U.S. District Court for the Northern District of Illinois last October — in which a trial court entered a judgment of $228 million.[9]

States Follow BIPA's Lead as Biometric Legislation Rises Nationwide

Additional states have enacted biometric privacy legislation, including Washington and Texas, following Illinois' lead.

Washington's biometric privacy law regulates companies' use, collection, storage and processing of biometric information.[10]

Similar to BIPA, Washington's biometric privacy law requires companies to provide notice to the individual whose data is collected, obtain consent from that individual and arrange a mechanism for preventing further use of the individual's biometric information for commercial purposes.[11]

Texas has also passed legislation regulating the collection of biometric information. Under the Texas Capture or Use of Biometric Identifier Act, or CUBI, companies may be liable for up to $25,000 per violation.[12]

CUBI regulates the capture, possession and retention of biometric identifiers, including retina or iris scans, fingerprints, voiceprints, or recordings of hand or face geometry.

Under CUBI, companies are required to provide notice before capturing biometric information, receive prior consent, protect the biometric information from disclosure using reasonable care, destroy the biometric information within a reasonable time, and refrain from selling or otherwise disclosing such information unless required or consented to for a specific purpose.[13]

Unlike BIPA's private right of enforcement, the Washington and Texas statutes can only be

enforced by the state's attorney general.

One of the Texas attorney general's first actions to enforce CUBI was filed against Facebook's parent company, Meta Platforms Inc., alleging that Meta unlawfully captured and retained facial geometry of both Meta users and nonusers.[14]

The suit seeks damages for at least 10 years' worth of violations, and an injunction to prevent Meta from collecting additional biometric information. The parties are currently undergoing discovery.

Other states, such as California, have integrated biometric information protection within their broader privacy laws.

For example, California's Consumer Privacy Act of 2018 includes biometric information within its broader definition of "personal information" and "sensitive personal information,"[15] and regulates such information by requiring companies to provide clear and transparent information relating to how they collect and process biometric information, and implement reasonable security procedures to protect the information.[16]

Municipalities have started regulating biometric information as well, including Portland, Oregon, and New York City. Portland was the first city in the country to ban use of facial recognition technology by private entities within the city.[17]

The ordinance is broadly structured and only excludes facial recognition use that relates to legal compliance, user verification by an individual to access their own electronic devices and automatic face detection services used in social media applications.

New York City's municipal ordinance is similar to BIPA and prohibits the use of biometric information for the purpose of selling or profiting from such information, and requires commercial establishments to notify customers of their collection of biometric information.[18] Both Portland and New York City provide a private right of action for residents to directly sue entities that violate the ordinances.

Somewhat uniquely, New York's ordinance provides for a 30-day notice-and-cure process prior to initiating an action — other than violations that include selling or otherwise profiting from the biometric information.[19]

Keeping an Eye Out: 2023 Biometric Privacy Law Proposals

Various states across the country, including Arizona,[20] Massachusetts,[21] Minnesota,[22] Maryland,[23] New York,[24] Oregon,[25] Tennessee,[26] Kentucky[27] and Hawaii,[28] have recently introduced legislative proposals relating to biometric information in 2023.

Each of the proposals regulates biometric information and, similar to BIPA, addresses procedures for the use, retention, and destruction of such information. Notably, each of the proposals, other than Kentucky, includes a private right of action for individuals to sue for violations.

Additionally, the Federal Trade Commission adopted a new policy statement on May 18, addressing biometric information regulation under Section 5 the FTC Act, which governs unfair and deceptive business practices.[29] The policy statement is the first substantial step taken by the FTC to regulate biometric information in over a decade.

In the policy statement, the FTC set forth an inexhaustive list of practices that the FTC intends to scrutinize to determine whether such practices are unfair or deceptive, including:

- Inter alia, false or unsubstantiated marketing claims relating to the reliability and accuracy of biometric information technology;
- Deceptive statements about a company's collection and use of biometric information; and
- Collection, retention and use of consumers' biometric information in a way that causes or is likely to cause substantial injury.

The FTC's recent statement signals that the FTC may start bringing enforcement actions against companies that improperly collect, develop or use biometric information.

A Handful of Tips to Comply With Biometric Privacy Regulation Requirements

The increase in biometric privacy class actions, coupled with the proliferation of proposed legislation, suggests that biometric compliance will be a top concern for businesses as they adopt new biometric tools and technology, and as those tools continue to evolve to meet the needs of personalization, volume and other commercial concerns.

The use of geogating, or location-based marketing to consumers, and similarly targeted technologies or practices to address compliance, will be increasingly outmoded as the patchwork of regulations evolves.

When collecting biometric information, ensure that your company is organized and transparent regarding its use, collection and retention.

Compliance programs should be carefully tailored both to the unique facts of each company's specific data collection programs and the requirements of the jurisdictions in which the company operates — which includes jurisdictions in which users of online applications are located.

At a minimum, companies should carefully consider implementing the following when collecting data that may be considered biometric information:

- Conspicuously provide written notice before collecting, using and storing any biometric information;
- Disclose your biometric information use, collection and retention methods within any employee agreements, privacy policies or terms of use;
- Obtain prior written consent from any individual who may be subject to the collection of their biometric information;
- Only collect biometric information to the extent such information is necessary to achieve a specific purpose;
- Store any collected biometric information securely; and

- Organize an internal mechanism for destroying biometric information once such information is no longer needed.

Joseph Wylie and Katherine Staba are partners, and Kelsi Robinson is an associate, at K&L Gates LLP.

[1] Over 100 class action suits alleging BIPA violations have been filed in 2023 thus far.

[2] See, e.g., In re Facebook Biometric Info. Priv. Litig., No. 15-CV-03747-JD (N.D. Cal. Feb. 26, 2021) (settling for $650 million); Rivera v. Google LLC, No. 2019-CH-00990 (Ill. Cir. Ct. Sept. 14, 2022) (settling for $100 million); Boone v. Snap Inc., No. 2022LA000708 (Ill. Cir. Ct. Nov. 22, 2022) (settling for $35 million).

[3] 740 Ill. Comp. Stat. Ann. 14/15 (West 2008).

[4] 740 Ill. Comp. Stat. Ann. 14/10 (West 2008).

[5] 740 Ill. Comp. Stat. Ann. 14/15 (West 2008).

[6] Id. § 15(e).

[7] 740 Ill. Comp. Stat. Ann. 14/20 (West 2008). Notably, the individual does not need to demonstrate actual harm or independent damages when suing based on a BIPA violation; the violation itself is considered adequate harm. See Cothron v. White Castle Sys., Inc., No. 128004, 2023 WL 2052410, at *7 (Ill. Feb. 17, 2023) (citing Rosenbach v. Six Flags, 129 N.E.3d 1197, 1206 (Ill. 2019)).

[8] Cothron, 2023 WL 2052410, at *8.

[9] Rogers v. BNSF Ry. Co., Case No. 19-CV-03083 (N.D. Ill. 2022). On 9 November 2022, BNSF filed a motion for a new trial under Rule 59(a) or to reduce the damages award under Rule 59(e). The posttrial briefing is currently under review.

[10] Wash. Rev. Code Ann. § 19.375.010 (West 2017).

[11] Wash. Rev. Code Ann. § 19.375.020 (West 2017).

[12] Tex. Bus. & Com. Code Ann. § 503.001 (West 2017).

[13] Id.

[14] Texas v. Meta Platforms, Inc., No. 22-0121 (Tex. Ct. [71st Dist.] 2022).

[15] Cal. Civ. Code § 1798.140.

[16] Cal. Civ. Code § 1798.100. California also introduced SB-1189, a BIPA-like biometric privacy regulation, in 2022. The regulation would create a private right of action against companies who fail to adhere to the act's requirements, which include displaying public written policies that establish a retention schedule for storage of biometric information, obtaining prior informed written consent, and refraining from selling or disclosing biometric information.

[17] Portland, Or., City Code §§ 34.10.010-34.10-050.

[18] N.Y.C., N.Y., Admin. Code §§ 22-1201-1205.

[19] Id.

[20] SB1238, introduced on 30 January 2023.

[21] HD.3053 and SD.2218, introduced on 20 January 2023.

[22] SF 954, introduced on 30 January 2023.

[23] SB0169, introduced on 20 January 2023.

[24] A1362, introduced on 17 January 2023.

[25] SB619, introduced on 9 January 2023.

[26] SB0339, introduced on 23 January 2023.

[27] House Bill 483, introduced on 21 February 2023.

[28] SB1085, introduced on 20 January 2023.

[29] See Fed. Trade Comm'n, Policy Statement of the Federal Trade Commission on Biometric Information and Section 5 of the Federal Trade Commission Act (May 18, 2023), https://www.ftc.gov/system/files/ftc_gov/pdf/p225402biometricpolicystatement.pdf.