Cybersecurity Law Report
An Acuris company

cslawreport.com

March 16, 2022

BIOMETRICS

No End in Sight: Biometrics Litigation Trends

By Elizabeth McGinn, Amanda Lawrence, Scott T. Sakiyama and Michael Rosenberg, *Buckley LLP*

Modern biometrics applications are myriad with more continually being developed. They allow users to unlock devices, make payments, detect theft, track time and much more. These applications are not overlooked by the plaintiffs' bar. Since 2019, more than 1,000 class action lawsuits have been filed under Illinois' Biometric Information Privacy Act (BIPA), and plaintiffs show no signs of slowing down. The public is also increasingly attuned to biometric privacy risks. The IRS, in response to an outcry last month, abandoned its plans to require facial recognition for online logins.

These are likely still the early innings of biometrics litigation and enforcement activity. Last month, Texas' attorney general entered the fray by filing suit against Facebook under Texas' own biometrics law. Illinois, Texas and Washington are the only states with standalone biometrics laws on the books, but at least 27 other states have introduced biometrics legislation.[1] Another 16 states and the District of Columbia address biometric privacy through existing privacy and data breach notification statutes.[2] Adding to the maze, companies must also be aware of city biometric laws passed in Portland, New York City and Baltimore.

The focus remains for now on BIPA, and for good reason: it is the only state law with a private right of action – and plaintiffs have pounced. BIPA applies to companies that collect, capture, purchase, obtain, disclose, or disseminate "biometrics identifiers," defined as "a retina or iris scan, fingerprint, voiceprint, or a scan of hand or face geometry," or "biometric information," 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." Companies subject to the law must:

- have a publicly available written biometrics policy;
- obtain an individual's written consent prior to collection; and
- otherwise comply with the statutory restrictions on biometric use, sale and storage.

The risks of non-compliance are steep: BIPA permits actual damages or liquidated damages of $1,000 for each negligent violation and $5,000 for each reckless or intentional violation, plus attorneys' fees and costs and injunctive relief.

See "Big Questions for BIPA Case Law in 2021" (Feb. 17, 2021); and "Complying With NYC's New Biometrics Law" (Aug. 11, 2021).

BIPA Lawsuits Besiege Big Tech

The pace of BIPA litigation and settlements has been relentless. Last year, Facebook settled a BIPA class action over its photo-tagging feature for $650 million, and TikTok settled for $92 million over face detection in videos. Microsoft, Google, IBM and others have not escaped scrutiny.

Bids to dismiss BIPA actions are commonly denied.[3] For example, in *Naughton v. Amazon*, Amazon moved to dismiss a class action alleging that Amazon collected the plaintiff's facial geometry without his consent – as part of a "wellness check" required for employees to enter a warehouse – and disclosed the data to third parties. First, the court rejected Amazon's argument that it did not take an "active step" in collecting the plaintiff's biometric data, noting that the plaintiff plausibly alleged that "Amazon itself implemented the facial scans and required workers to submit to these scans as a condition of work." Second, the court held that the plaintiff adequately alleged Amazon's possession of biometric information under BIPA Sections 15(a) and 15(d), given its alleged active step of collecting and storing the biometric data. Moreover, the court held that the plaintiff adequately alleged that Amazon "plausibl[y] disseminat[ed]" the data to third parties under Section 15(d).

Courts have similarly rejected challenges to BIPA claims involving voiceprints and other biometrics modalities. In *Carpenter v. McDonald's Corp.*, the plaintiff alleged that in certain drive-through locations, McDonald's deploys AI technology that collects customers' voiceprints without their consent, in order "to correctly interpret customer orders and identify repeat customers to provide a tailored experience." McDonald's denied that its voice technology extracts biometrics, arguing that it merely synthesizes information necessary to discern a customer's intent, analyzing speaker characteristics such as accents, speech patterns, gender and age. The court held that the plaintiff adequately alleged that McDonald's can identify unique customers through mechanical voice analysis, and, therefore, that it "collects voiceprints." As in Naughton, the court quickly dispensed with arguments made by McDonald's that it did not take an "active step" in collecting the data, and that McDonald's lacked possession of the data.

See "Illinois Federal Court Denies Standing in BIPA Claim Against Google" (Jan. 23, 2019).

Plaintiffs Target Wide-Ranging Businesses and Technologies

The headlines focus on BIPA's impact on big tech, but small and medium-size businesses have not been spared. Employers' collection of fingerprint scans or other biometrics to aid in security and time tracking continues to pose significant risk under BIPA. Various other biometrics applications, including the following, are also under fire, crystallizing the need for adequate compliance across industries.

Driver Monitoring

Transportation and logistics companies are defending BIPA claims alleging that their dashcams collect, and sometimes sell or trade, drivers' biometric data without notice or consent.[4] Automakers face similar claims that

advanced driver assistance systems unlawfully scan and process drivers' facial geometries in order to monitor and control drivers' behavior. Future vehicles are likely to implement enhanced face and gesture recognition, exposing automakers and their affiliates to ongoing biometrics risk.

Video Surveillance

Retail establishments and other businesses have been accused of unlawfully scanning the facial geometry of customers and cross-referencing that data with stored biometrics from prior customer visits, as alleged in lawsuits against Home Depot, Lowe's and an Illinois casino. Macy's and others are separately alleged to have used a database assembled by Clearview AI, which allegedly scraped billions of facial geometries off the internet, allowing retailers to identify customers from store surveillance footage. These cases serve as reminders for businesses to consider the sources of their underlying data, obtain and document the required consents, and carefully weigh the risks associated with using facial recognition technology.

Remote Proctoring

Online exam technology has proliferated during the pandemic, and so have corresponding lawsuits. Colleges, universities and their affiliates, however, have a potent defensive weapon: BIPA's exemption of "financial institutions" subject to the GLBA. In *Doe v. Northwestern*, a student alleged that Northwestern's remote tools effectively surveil online test-takers by capturing, using and storing "vast amounts of data, including [facial data], recorded patterns of keystrokes, eye monitoring data, gaze monitoring data, and camera and microphone recordings." Northwestern moved to dismiss, relying upon the "financial institution" exemption, and the court granted its motion on February 22, 2022. The court held that the GLBA broadly defines "financial institutions" to include "any institution the business of which is engaging in financial activities," and credited the FTC's Privacy Rule that considers colleges and universities to be financial institutions where they "appear to be significantly engaged in lending funds to consumers." Northwestern's software provider, Examity, relied on the same BIPA exemption in a separate action, as an "affiliate" of a financial institution subject to the GLBA.

See CSLR's two-part series on the intelligent workplace in the age of a pandemic: "Balancing Innovation and Risk" (Oct. 28, 2020); and "Six Privacy and Security Safeguards" (Nov. 11, 2020).

All Eyes on the Illinois Supreme Court

Since the Illinois' Supreme Court's seminal 2019 decision in *Rosenbach v. Six Flags Entm't Corp.* – widely seen as opening the BIPA floodgates – courts have steadily stripped away companies' defenses against BIPA claims. Multiple cases pending before the Illinois Supreme Court will determine if they dwindle further.

See "Implications of the Illinois Supreme Court's BIPA Holding Against Six Flags" (Feb. 20, 2019).

Workers' Compensation Act Preemption

Employers had hoped to avoid BIPA liability by claiming that the Illinois Workers' Compensation Act (IWCA) is the exclusive remedy for employee injury claims. On February 3, 2022, in *McDonald v. Symphony Bronzeville Park LLC*, the Illinois Supreme Court rejected preemption, as "the personal and societal injuries caused by violating [BIPA's] prophylactic requirements are different in nature and scope from the physical and psychological work injuries that are compensable under the [IWCA]." The court also determined that the legislature specifically intended BIPA claims to arise in the employment context, noting that BIPA defines "written release" to include "a release executed by an employee as a condition of employment."

Statute of Limitations

BIPA does not specify a statute of limitations, and the Illinois Supreme Court is finally set to address the issue. Last year in *Tims v. Black Horse Carriers*, the Illinois Appellate Court held that the applicable time period varies by section: BIPA claims relating to informed consent, data retention policy disclosure and safeguarding (claims under sections 15(a), 15(b) and 15(e)) are subject to a five-year "catch-all" statute of limitations, while claims based on unlawful profit or disclosure (claims under sections 15(c) and 15(d)) are subject to a one-year statute of limitations. This ruling, if left to stand, would permit most BIPA actions, which allege violations of multiple subsections, to proceed as timely. On January 26, 2022, the Illinois Supreme Court granted leave to appeal in Tims.

Accrual of Claims

Another heavily litigated – and enormously consequential – issue is whether each biometric scan restarts the clock on the statute of limitations and counts as a separate violation (and penalty). The Seventh Circuit certified this question to the Illinois Supreme Court in *Cothron v. White Castle* on December 20, 2021. White Castle argued that the Illinois' Single Publication Act – which limits plaintiffs to "one cause of action" for privacy damages founded upon any "single publication" – should apply to BIPA claim accrual. The Seventh Circuit found support for White Castle's position in *West Bend Insurance v. Krishna Shauberg Tan, Inc.*, in which the Illinois Supreme Court held that a biometric disclosure to a third party was a "publication" for the purpose of determining insurance coverage. However, the Seventh Circuit stated that it was "genuinely uncertain" about the answer, and that "only the state's highest court can provide authoritative guidance."

See "Navigating Today's Biometric Landscape" (Apr. 3, 2019).

BIPA Standing: Plaintiffs Hold All the Cards

Rosenbach made clear that plaintiffs need only allege a technical BIPA violation, and not actual harm, to bring a BIPA claim in state court. To remove such cases to federal court, defendants must argue – unenviably – that the plaintiffs have alleged an injury-in-fact and, therefore, have standing under Article III. That task has become more difficult in light of *Thornley v. Clearview AI*, in which the Seventh Circuit affirmed that plaintiffs are entitled to plead around Article III and remain in state court. There, the complaint asserted only a violation

of BIPA Section 15(c), which prohibits a private entity from profiting from biometric data, and specifically pleaded that no plaintiff or putative class member "suffered ***any*** injury as a result of the [BIPA] violations other than the statutory aggrievement…." Accordingly, the plaintiffs argued they lacked Article III standing in order to remand the case to state court.

Judge Wood's majority opinion distinguished earlier Seventh Circuit standing cases, including *Fox v. Dakkota Integrated Sys.*, which alleged an employer violated Section 15(a) by failing to comply with its data retention and destruction policies. There, the court affirmed that an unlawful retention of biometrics is "as concrete and particularized an injury" as an unlawful collection of biometrics. But "allegations [of injury] matter," and in *Thornley*, the court gave dispositive weight to their absence, as standing depends on both "what [the] section provides and what the plaintiff has alleged." Accordingly, defendants should anticipate artful pleading and carefully consider BIPA plaintiffs' alleged injuries – or lack thereof.

See "Illinois Appellate Decision Creates Split on Standing to Sue Under BIPA" (Dec. 12, 2018).

Practice Tips

Companies should not expect the courts to curtail BIPA's reach. That path goes through the Illinois legislature – and recent bills to rein in BIPA have stalled.[5] Instead, companies should ensure their biometrics collection practices are compliant on an ongoing basis. As biometrics technologies and applications evolve, plaintiffs' BIPA claims will mirror those changes.

To comply with BIPA and emerging biometrics laws, companies must:

- adopt written, publicly available policies and procedures;
- properly disclose details about the collection, use, storage, retention and dissemination of the data;
- obtain written consent prior to collection;
- establish guidelines for destroying the data after the initial purpose of the collection has been achieved, or if it has been three years since the last transaction.

Potential vulnerabilities in vendors' handling of biometrics must also be addressed. Contracts should stipulate that vendors will adhere to the highest standards in processing biometric data, through privacy and security risk assessments, encryption and other safeguards.

The past few years have highlighted the promise and perils of biometrics collection. With transparency and care, companies can implement innovative biometrics policies to benefit customers – while keeping litigation and enforcement activity at bay.

See "Six Ways to Address Privacy Concerns in Biometric Vendor Contracts" (Mar. 3, 2021).

Elizabeth E. McGinn is a partner in the Washington, D.C., and New York offices of Buckley LLP. She focuses her practice on assisting clients in identifying, evaluating and managing the risks associated with cybersecurity, internal privacy and information security practices, as well as those of third-party vendors. A significant part of her practice involves addressing data security breaches, working proactively with clients to prevent data security breaches and responding to regulatory inquiries, investigations and enforcement actions related to privacy, information security and cybersecurity issues.

Amanda R. Lawrence is a partner in the firm's Washington, D.C., office where she assists clients in managing cybersecurity, privacy, information security and vendor risks and compliance, as well as evaluating and addressing potential data security incidents, including drafting consumer and regulator notifications. She has a focus on financial services industry issues, including privacy, cybersecurity, data breach, class actions and FTC and other regulator priorities.

Scott T. Sakiyama is a partner in the firm's Chicago office. He represents clients in a wide range of enforcement and litigation matters. His work includes litigation throughout the country in cases involving federal and state consumer protection statutes as well complex commercial disputes. He also regularly represents clients in enforcement matters before federal and state agencies including the Consumer Financial Protection Bureau, the Department of Justice, the FTC and state attorneys general.

Michael M. Rosenberg is an associate in the firm's Chicago office. He advises clients on consumer financial services, privacy and cybersecurity-related matters and electronic discovery.

[1] 2021 AL H.B. 216 (Alabama); 2021 AK S.B. 116 (Alaska); 2021 CO H.B. 1244, S.B. 190 (Colorado); 2021 CT S.B. 893 (Connecticut); 2021 FL H.B. 969 (Florida); 2021 HI S.B. 1009 (Hawaii); 2020 IN H.B. 1371 (Indiana); 2021 KY S.B. 280 § 2(5), 2022 KY H.B. 32 (Kentucky); 2021 ME S.P. 535 (Maine); 2021 MD S.B. 16, 2022 MD H.B. 259 (Maryland); 2021 SD.1726, 2022 S.2667 (Massachusetts); 2021 MS S.B. 2612 (Mississippi); 2022 MO H.B. 2716 (Missouri); 2021 MN S.F. 1408 (Minnesota); 2021 MT H.B. 710 (Montana); 2020 NJ A.B. 3625 (New Jersey); 2021 NY A.B. 27 (New York); 2021 NC S.B. 569 (North Carolina); 2021 OK H.B. 1602 (Oklahoma); 2021 PA H.B. 5945 (Pennsylvania); 2019 RI H.B. 5945, 2019 RI S.B. 234 (Rhode Island); 2021 SC H.B. 3063 (South Carolina); 2021 UT S.B. 200 (Utah); 2020 VA H.B. 2307 (Virginia); 2021 WA H.B. 1433 (Washington); 2021 WV H.B. 2064, 2021 WV H.B. 3159 (West Virginia); 2019 WI S.B. 851 (Wisconsin).

[2] Cal. Civ. Code § 1798.100 (California); Del. Code 6, § 12B-100 (Delaware); D.C. Code § 28-3851 (District of Columbia); 2021 ID H.B. 147 (Idaho); Iowa Code § 715C.1(11)(a), 2018 IA H.F. 39 (Iowa); La. Stat. Ann. § 51:3071-51:3077 (Louisiana); Neb. Rev. Stat. § 87-803 (Nebraska); Nev. Rev. Stat. § 629.161 (Nevada); NMSA 1978, §§ 57-12C-1 et seq. (New Mexico); 2021 NH H.B. 597 (New Hampshire); ND S.B. 2075 (North Dakota); Ohio Rev. Code. § 3965.01 (Ohio); Or. Rev. Stat. § 646A.604 (Oregon); TN H.B. 766 § 1 (Tennessee); Vt. Stat. Ann. 9 § 2430 (Vermont); Wyo. Stat. Ann. § 6-3-901, Wyo. Stat. Ann. § 40-12-501 (Wyoming).

[3] *See, e.g., Microsoft Corp*, 525 F. Supp. 3d at 1300 (denying motion as to 15(c) claim)); *Rivera*, 238 F. Supp. at 1091 (denying motion in full); *Int'l Bus. Machines Corp.*, 2020 WL 5530134, at *1 (denying motion as to five of seven counts); *In re Clearview AI, Inc., Consumer Priv. Litig.*, No. 21-CV-0135, 2022 WL 444135, at *12 (N.D. Ill. Feb. 14, 2022) (denying motion as to BIPA claims); *Naughton v. Amazon.com, Inc.*, No. 20-CV-6485, 2022 WL 19324, at *1 (N.D. Ill. Jan. 3, 2022) (denying motion in full).

[4] *Arendt et al. v. Netradyne Inc.*, No. 22-cv-00749 (N.D. Ill. 2022); *Hernandez v. Omnitracs, LLC*, No. 22-cv-00109 (N.D. Ill. 2022); *Lewis v Maverick Transportation LLC*, et al., No. 22-cv-00046 (S.D. Ill. 2022).

[5] *See* IL House Bills 559, 560.