Cybersecurity Law Report cslawreport.com

Mar. 8, 2023

Biometrics

BIPA Decisions Expand Potential Liability: What's Next in Illinois and Other States?

By Justine Gottshall and Benjamin Stein, *InfoLawGroup*

In two long-awaited decisions, the Illinois Supreme Court determined that all claims under Illinois' Biometric Information Privacy Act (BIPA) are subject to a five-year statute of limitations and a separate claim accrues each time an entity scans or transmits an individual's biometric identifier or biometric information. This article analyzes theses outcomes, and addresses other developments and enforcement actions under state and local biometrics laws around the country.

See our two-part series on shaping the BIPA landscape: "Notable Trends and Developments" (Sep. 7, 2022); and "Avoiding Liability" (Sep. 14, 2022).

Illinois' BIPA: Every Scan and Every Disclosure (or Redisclosure) Is an Independent Violation

In February 2023, the Illinois Supreme Court issued its long-awaited decision in the closely watched *Cothron v. White Castle System, Inc.* case. *Cothron* had been the most anxiously watched BIPA case in recent years and the result is sure to thrill potential BIPA plaintiffs (and their counsel), while terrifying businesses operating in the state.

The case was before the Illinois Supreme Court (Court) to answer a question certified to it by the Seventh Circuit and had been pending since December 2021. The question, paraphrased to add context was:

"Do …. claims [under BIPA Section 15(b), which prohibits the collection of biometric identifiers/information without first providing notice and securing the subject's written consent, and BIPA Section 15(d), which similarly prohibits the disclosure, redisclosure, or other dissemination of that biometric data without first securing the subject's consent] accrue each time a private entity scans a person's biometric identifier and each time a private entity transmits such a scan to a third party, respectively, or only upon the first scan and first transmission?"

See "No End in Sight: Biometrics Litigation Trends" (Mar. 16, 2022).

Plaintiff Asserted More Than a Decade of Violations

Plaintiff manages a White Castle restaurant, where she's worked since 2004. According to the complaint, not long after she started working there, White Castle introduced a fingerprint-based access system whereby employees were required to scan a fingerprint to access their pay stubs and computers. The scans were transmitted to and verified by White Castle's third-party vendor before the employee was granted access.

While BIPA took effect in 2008, Cothron asserted that White Castle did not seek her consent to its fingerprint-scanning practices until 2018, thereby violating BIPA for more than a decade. She sought to represent a class of similarly situated White Castle employees in Illinois, a class that White Castle estimated could comprise as many as 9500 individuals.

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

District Court Sided With Plaintiff, Seventh Circuit Certified Question to Supreme Court

At the District Court, White Castle moved for judgment on the pleadings. It argued that plaintiff's action was time-barred because her claim accrued in 2008, the first time White Castle collected and disclosed her fingerprint to its vendor after BIPA became effective. Plaintiff countered that a new violation and claim occurred each time her fingerprint was scanned and disclosed to the authentication vendor, and thus she could bring claims for each scan that took place within the relevant statute of limitations for BIPA claims. (More on that issue in the discussion of the *Tims* case, immediately below.)

The District Court sided with plaintiff. White Castle sought and received an interlocutory appeal to the Seventh Circuit. The Seventh Circuit, finding both parties' interpretations of when claims accrued reasonable under Illinois law, certified the question to the Illinois Supreme Court.

White Castle Argued Claim Only Accrues on First Scan or Transmission

On the issue of when a claim related to collection accrues, the thrust of White Castle's argument regarding Section 15(b), as described in the Court's opinion, was that the phrase "unless it first" refers to a singular point in time – *i.e.*, that notice and consent must precede collection. White Castle further argued that the active verbs used in section 15(b) – collect, capture, purchase, receive, and obtain – all mean to gain control, an action that can only happen once under the plain meaning of those terms.

Similarly, White Castle argued that a violation of 15(d) could only occur upon disclosure of biometric data to a new third party – not to the repetitive disclosure of the same biometric identifier from the same individual to the same third-party recipient.

Supreme Court Concludes Claim Accrues at Each Act

The Court (in a 4-3 opinion) concluded that, based on the plain language of the relevant BIPA sections, claims accrue at each act of collection and each act of disclosure, respectively – even if collecting the same biometric identifier and transferring it to the same third party in each instance.

After parsing the statutory language, the Court concluded that White Castle's interpretation had no merit: "We believe that the plain language of section 15(b) and 15(d) demonstrates that such violations occur with every scan or transmission."

It then went on to reject other, non-textual arguments made by White Castle (and the *amici* groups siding with it) in support of its interpretation that a claim could accrue only at first collection or first disclosure, including an argument that holding each scan or each disclosure to generate its own claim "could potentially result in punitive and 'astronomical' damage awards that would constitute 'annihilative liability' not contemplated by the legislature" because of BIPA's statutory-damage provisions.

Section 20 of BIPA provides that an aggrieved party "may recover for each violation" $1,000 for negligent violations or $5,000 for intentional ones (among other things). Based on this provision White Castle estimated that its potential liability could exceed $17 billion. Unswayed by this concern, the Court concluded that "[u]ltimately … we continue to believe that policy-based concerns about potentially excessive damage awards under [BIPA] are best addressed by the legislature."

Illinois' BIPA: All Claims are Subject to a Five-Year Statute of Limitations

Also in February 2023, the Illinois Supreme Court issued its opinion in a second closely watched BIPA case: *Tims v. Black Horse Carriers, Inc.* At issue in *Tims* was the appropriate statute of limitations for claims under various sections of BIPA, including the collection and disclosure provisions discussed above in connection with *Cothron*.

Alleged BIPA Violations

In *Tims*, the plaintiff – a former employee of defendant Black Horse – alleged that defendant required employees to use a fingerprint-based time clock. Tims claimed that Black Horse violated BIPA because "it (1) failed to institute, maintain, and adhere to a publicly available biometric information retention and destruction policy required under section 15(a); (2) failed to provide notice and to obtain his consent when collecting his biometrics, in violation of section 15(b); and (3) disclosed or otherwise disseminated his biometric information to third parties without consent in violation of section 15(d)."

See "Big Questions for BIPA Case Law in 2021" (Feb. 17, 2021).

Five-Year Versus One-Year SOL

As in *Cothron*, the dispute that brought the case to the Illinois Supreme Court centered on the timeliness of Tims' claims: BIPA lacks its own statute of limitations and the parties in *Tims* disagreed over what limitations provision should apply.

Defendant's position was that the one-year limitation period set out under Section 13-201 of the Illinois Statutes for defamation and similar privacy-related actions should apply to BIPA. Section 13-201 reads: "Actions for slander, libel or for publication of matter violating the right of privacy, shall be commenced within one year next after the cause of action accrued."

Tims argued instead that Section 13-205's catch-all five-year limitation period should apply to BIPA. Section 13-205 reads, in relevant part, that "all civil actions not otherwise provided for, shall be commenced within 5 years next after the cause of action accrued." Tims argued that, because BIPA claims do not involve the publication of biometric data and because BIPA was not intended "to regulate the publication of biometric data," the one-year limitations period should not apply.

Appellate Court Split the Baby

Before this case reached the Illinois Supreme Court, the Illinois Appellate Court – in an apparent nod to the Judgment of Solomon – split the baby. It held in 2021 that the disclosure provision of BIPA (discussed above) and Section 15(c) of BIPA – which prohibits an entity in possession of biometric identifiers/information from selling, leasing, trading or otherwise profiting from that information – were publication-based claims subject to the one-year limitations provision. Other BIPA claims (including collection without consent under Section 15(b) and failure to adopt and publish a retention policy for biometric information under Section 15(a)) were not inherently related to publication or dissemination of biometric information and were therefore subject to the five-year limitations period.

Supreme Court Weighs In on Appellate Court's Error

On appeal, the Court held that the appellate court erred in applying two different limitation periods to BIPA – a conclusion advocated for by both parties to the case. After acknowledging that the sections of BIPA prohibiting sale of biometric information (15(c)) or disclosure of that information without consent (15(d)) contain language that "could be defined as publication," the Court nevertheless concluded that "when we consider not just the plain language of section 15 but also the intent of the legislature, the purposes to be achieved by the statute, and the fact that there is no limitations period in the Act, we find that it would be best to apply the five-year catchall limitations period codified in section 13-205" and that "[t]his would also further our goal of ensuring certainty and predictability in the administration of limitations periods that apply to causes of actions under the Act."

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

Illinois' BIPA: But Maybe, Just Maybe, You're an Exempt Financial Institution?

BIPA includes a small handful of express exemptions, most narrow enough that they do not generate much discussion. However, one of these exemptions – which renders BIPA's provisions inapplicable to any "financial institution or an affiliate of a financial institution that is subject to Title V of the federal Gramm-Leach-Bliley Act" (GLBA) – has been wielded creatively recently to help colleges and universities escape BIPA claims early in the litigation process.

Under the GLBA, "financial institution" means "any institution the business of which is engaging in financial activities." In the last year, Northwestern University, DePaul University, and a handful of other Illinois colleges and universities have all argued successfully that they are a "financial institution" for GLBA purposes – and thereby exempt from BIPA requirements – based on the fact that they make and administer student loans through participation the Department of Education's Federal Student Aid program.

In granting motions to dismiss in these cases, the courts routinely rejected arguments that the educational institutions should remain subject to BIPA because they were primarily engaged in the business of higher education – and not financial activities. While this GLBA exemption may not be useful to a huge swath of potential BIPA defendants, it is clearly worth noting for businesses subject to GLBA – even where the business may not be primarily or traditionally a financial institution.

See "Biometric Data Protection Laws and Litigation Strategies (Part One of Two)" (Jan. 31, 2018); Part Two (Feb. 14, 2018).

So, Where Are We in Illinois?

As a refresher, BIPA regulates "biometric identifiers" – meaning "a retina or iris scan, fingerprint, voiceprint, or scan of hand or face geometry" (subject to some exceptions not relevant to the cases discussed in this article) – as well as "biometric information" – meaning "any information, regardless of how it is captured, converted, stored, or shared, based on an individual's biometric identifier used to identify an individual."

Under current Illinois law, every scan (collection, capture, receipt, etc.) of a biometric identifier or biometric information and every disclosure now constitutes the accrual of a new claim and the limitations period for all BIPA claims is five years. Taken together, and with the existing draconian damages and fee-shifting provisions in BIPA, there is now more incentive than ever for plaintiffs to bring BIPA claims. Early attempts to dismiss on timeliness grounds will be harder to win, classes will be larger, and potential damage calculations will be enormous.

Any party collecting or receiving biometric identifiers or information from Illinois residents should already have been plenty concerned about ensuring their BIPA compliance efforts were entirely buttoned-up based on the years of high-volume, high-stakes litigation leading up to this point.

While there may be some narrow exceptions, unless a company clearly falls under one, its cause for concern has just been magnified exponentially. And, while the Illinois legislature is considering modifications to BIPA, there is no guarantee that any weakening amendments will be adopted.

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

Texas: It Begins

Texas has, since 2009, had in place the Capture or Use of Biometric Identifiers Act (CUBI) which, among other things, prohibits the collection of biometric identifiers (defined as any "retina or iris scan, fingerprint, voiceprint, or record of hand or face geometry") for a "commercial purpose" (which is not defined in the statute) without informing the subject and receiving consent.

Unlike BIPA, CUBI has no private right of action and the historical lack of enforcement by Texas' Attorney General has generally left it to live in the shadow of BIPA.

No longer. In February 2022, Texas Attorney General Ken Paxton sued Facebook and Instagram parent Meta for allegedly violating CUBI through facial-recognition processes that powered the "Tag Suggestions" feature offered by Facebook between 2010 and 2021 (the same conduct that drove Facebook's $650M BIPA settlement with a class of Illinois users**),** as well as allegedly subjecting all photos uploaded to Instagram to facial recognition. That litigation remains ongoing.

In October of 2022, AG Paxton followed up by bringing a second CUBI suit against Google over allegedly unlawful collection of biometric identifiers through facial-recognition features in its Google Photos service and its Nest Hub Max product, as well as through the alleged creation of voiceprints from recordings made by the Google Assistant service. That litigation remains ongoing as well, with a Google filing from mid-January providing a rather full-throated assault on the purported insufficiency of the claims made in the Attorney General's complaint.

While CUBI enforcement actions out of Texas remain a ripple compared to the deluge of BIPA cases brought over the last five plus years (a trend certain to at least continue following the *Cothron* and *Tims* decisions), these actions against Meta and Google should be a reminder that failure to consider compliance with Texas' law also carries risks (perhaps particularly – though hardly exclusively – for large technology companies).

Portland: It Begins?

Almost two years ago, Portland, Oregon, enacted a first-of-its-kind, city-level prohibition on the use of facial-recognition technology by private entities. In general, Portland's ban:

- applies broadly to use of facial-recognition technology by private entities (essentially, any non-government actor) at a place of public accommodation within the City of Portland, excluding private residences, *bona fide* clubs, or other non-public institutions;

- has very limited exceptions where use is necessary to comply with law, for verification purposes to access personal or employer-issued electronic devices, and "in automatic face detection services in social media applications;" and
- includes a private right of action and a drastic penalty provision, under which those injured by violation of the ordinance may recover the greater of actual damages or $1,000 per day for each day of a violation, plus attorneys' fees.

Against that background, two plaintiffs looking to represent a class of Portland residents sued Idaho-based convenience store chain Jacksons Food Stores in December 2022 – in what is seemingly the first action brought under Portland's ordinance.

Per the complaint, at three of Jacksons' stores in Portland, customers attempting to enter are made to look into a security camera, which scans their facial features and compares the result to a repository of facial-mapping data for blacklisted persons. Those who have been blacklisted are denied entry to the store. Those who pass the screening may enter.

Should it have made it to adjudication on the merits, this case may have provided an interesting opportunity to better understand the nuances of Portland's law – like how the "per day" measure of damages would have been calculated (e.g., $1,000 per class member for each day the system was in place or only for days on which a particular class member actually encountered the facial-recognition system? And, if the latter, would class certification even have been feasible?).

However, the case was quickly voluntarily dismissed (without prejudice) near the end of January 2023, and so we will have to wait for answers to those questions.

Baltimore: It Ends

Finally, on the opposite end of the spectrum, a city ordinance in Baltimore enacted in 2021 that prohibited the use of "face surveillance" by any actor within city limits expired pursuant to its own sunset provision as of December 31, 2022. As of the date of this writing, the City Council has yet to enact any successor ordinance.

What's Next?

Litigation, regulation and risks associated with biometric data are certain to continue to increase as multiple states consider legislation to regulate biometrics, plaintiffs' attorneys have success in bringing cases, and technology that could create liability proliferates. Biometrics are also subject to certain regulation under some of the new overarching state privacy laws (such as the California Privacy Protection Act as amended by the California Privacy Rights Act). Any company engaging in any activity that could potentially trigger biometrics issues should look carefully at the technology being used and all potential liability and compliance options. The risks are just too great to ignore.

Justine Young Gottshall is co-managing partner of the InfoLawGroup, a nationally recognized boutique firm practicing in the areas of privacy, data security, technology and advertising. She has assisted some of the largest companies in the world with their privacy and data security issues. Gottshall has served as an outside chief privacy officer for clients and she created the firm's CPO on Demand™ service.

Benjamin Stein is a partner with InfoLawGroup. In addition to extensive experience advising on compliance with biometrics laws, he also routinely counsels clients on: the Children's Online Privacy Protection Act, mobile marketing compliance, operating sweepstakes and contests, complex loyalty programs, subscription programs, influencer marketing campaigns, gift-card programs, and referral programs, as well as all manner of advertising- and technology-related issues and agreements.