Liability for Violating the Illinois Biometric Privacy Law: The *White Castle* Stands

By Judge James E. Snyder (ret.)

In February 2023, the Illinois Supreme Court weighed in on the Illinois Biometric Privacy Act (BIPA) in *Cothron v. White Castle System, Inc.,* 2023 IL 128004 (Rehearing denied July 18, 2023). Counsel to business clients and litigators should be aware of *Cothron,* the compliance requirements of regulation, and the possibility of substantial liability for violating BIPA.

In *Cothron,* the Illinois Supreme Court held that a claim of violation of the Act accrues 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. *Pg.* 2. Although the Court denied a request for rehearing in July, it issued a modified opinion including a dissent. *Pg.* 15.

Illinois has the country's first and most comprehensive regulation on collecting, storing, and disseminating biometric information. Other states include California, Florida, Texas, Washington, and, in some contexts such as data breaches, Alaska. Rulings in California suggest that, like Illinois-based claims, California may see nationwide class action claims. California claims for unauthorized biometric data collection or dissemination are based on that state's Unfair Competition Law, the closest analogue to the Illinois BIPA, as well as the California Constitution's Right to Privacy and a common law right to publicity. *Renderos et al. v. Clearview AI, Inc.,* Sup. Ct. Alameda Cty., RG21096898.

Illinois enacted BIPA in 2008. It mainly regulates private entities in the commercial context. Legislative findings highlighted that biometric data collection puts individuals "at heightened risk for identity theft," noting that when a person's data is compromised, the individual "has no recourse." The General Assembly determined that "an overwhelming majority of members of the public are leery of the use of biometrics" and that the "ramifications of biometric technology are not fully known." 740 ILCS 14/5. The Act's stated intent is to serve "public welfare, security and safety" by regulating the collection and use of biometrics. 740 ILCS 14/5 (g). The Act defines biometric identifiers (Sec. 10), regulates their use (Sec. 15), and creates a private right of action for violation (Sec. 20).

Biometric Identifiers Defined

It is perhaps an effort to define what is "biometric" and is distinct from traditional identifiers of perception and recognition. Section 10 of the Act includes the first statutory definition of biometric identifiers in the country. 740 ILCS 14/10. The legislature distinguished biometric identifiers from other unique identifiers, such as Social Security numbers.

A biometric identifier is biologically unique and immutable to a person. Biometric identifiers include retina and iris scans, voiceprints, and scans of hand or face geometry. This includes fingerprint identification through optical scan and through traditional ink pad methods. Biometrics do not, however, include writing samples, written signatures, photographs, demographic data, tattoo descriptions, or physical descriptions such as height, weight, hair color, or eye color.

Data may be biometric but not regulated by BIPA. For example, while most imaging and sampling collected for health care treatment or diagnosis may seem biometric (e.g., human biological samples used for scientific testing or screening, X-ray, MRI, and mammography), dissemination of such data is restricted by other state and federal regulations but is exempted from BIPA's definition of biometric information.

Although a traditional photograph of a person is not considered biometric data under the Act, courts have held that face geometry data collected from photographs or cloud-based photo data is covered biometric data. For example, in *Rivera v. Google*, the plaintiff's claim centered on digital photographs of her taken by use of a Google Droid camera and uploaded to a cloud-based system, Google Photos. *Rivera v. Google, Inc.* 238 F. Supp. 3d 1088 (N.D. Ill. 2017). Google captured her facial feature data to create a "face template" without her consent. The district court held that this constituted biometric identifier collection under the Act. *Rivera v Google, Inc. Pg.* 1090. Or consider *Clearview AI, Inc. Consumer Privacy Litig.,* 585 F. Supp. 3d 111. That case involved a claim that defendants "scraped' over three billion photographs from the

internet and used artificial intelligence algorithms to scan her facial geometry to create a marketable facial recognition database, which included her. The court held that scraping or collecting face geometry data from publicly available photo images on the internet can constitute the collection of non-public biometric data. *Pg*. 1123.

Although comprehensive, BIPA's definition of biometric identifiers does not address private biological sample collection in contexts such as paternity testing, social genealogical research, or anatomical gifts. But the Act casts a broad regulatory intent. The scale and ingenuity of these technologies is changing more rapidly than anyone can see presently.

Possessing, Collecting, and Disseminating Biometric Identifiers

Section 15 (a) Possession: A private entity in possession of biometric data must have a written policy made available to the public regarding its collection, storage, and destruction and must adhere to that policy. The policy must have a retention schedule and guidelines for permanently destroying the data within three years of the individual's last interaction with the private entity. It is not hard to imagine businesses coming into possession of such data being unaware of this requirement or needing the assistance of counsel to comply with the statute.

Section 15(b) Collection: A private entity may not "collect, capture, purchase, receive through trade, or otherwise obtain" a person's biometric data without first providing notice to and receiving consent from the person. While this is often called a prohibition on collection of data, Section 15(b) is broader. Like 15 (a), it regulates the possession of biometric data; however, the entity obtained the data, including information collected by third parties. The entity must inform each "subject" (person from whom the data was collected) that collection or storage has taken place, the purpose of the data collection, and receive "a written release executed by the subject." The statute's use of the term "release" appears to be a type of written consent.

Section 15(d) Dissemination: A private entity may not "disclose, redisclose, or otherwise disseminate" biometric data without consent. Once collected and stored in an electronic format, biometric data can easily be copied, transmitted, or received by additional parties, over and over again.

Extent of Relief

Section 20 Cause of Action: BIPA creates an individual right of action. 740 ILCS 14/20. Remedies include $1,000 or actual damages against a party that negligently violates the Act, or $5,000, or actual damages, for an intentional violation, plus attorney fees and costs as well as injunctive relief.

Tims v. Blackhorse Carriers, Inc. and the Statute of Limitations

Earlier in the same term, the Illinois Supreme Court determined that all claims under BIPA are subject to a five-year limitations period, *Tims v. Black Horse Carriers, Inc.* 2023 IL 127801. They reversed an Illinois Appellate Court finding that the one-year limitation period of Illinois Code of Civil Procedure Section 13-20 applied to claims based on publication, Sections 15 (a), (b) and (d). Applying a five-year limitation period to an employee class action indicated a wide scope of potential plaintiffs in cases like *Tims*.

Cothron v. White Castle System Inc. and Claim Accrual

Cothron focused on the nature and extent of Section 20 relief. The plaintiff claimed that her employer, White Castle, had collected and scanned her fingerprints each time she accessed her paystub or computer. She claimed that her employer had disseminated that biometric data to a third-party vendor that operated a verification system. She alleged that the dissemination occurred regularly during years that the Act had been in effect, perhaps thousands of times.

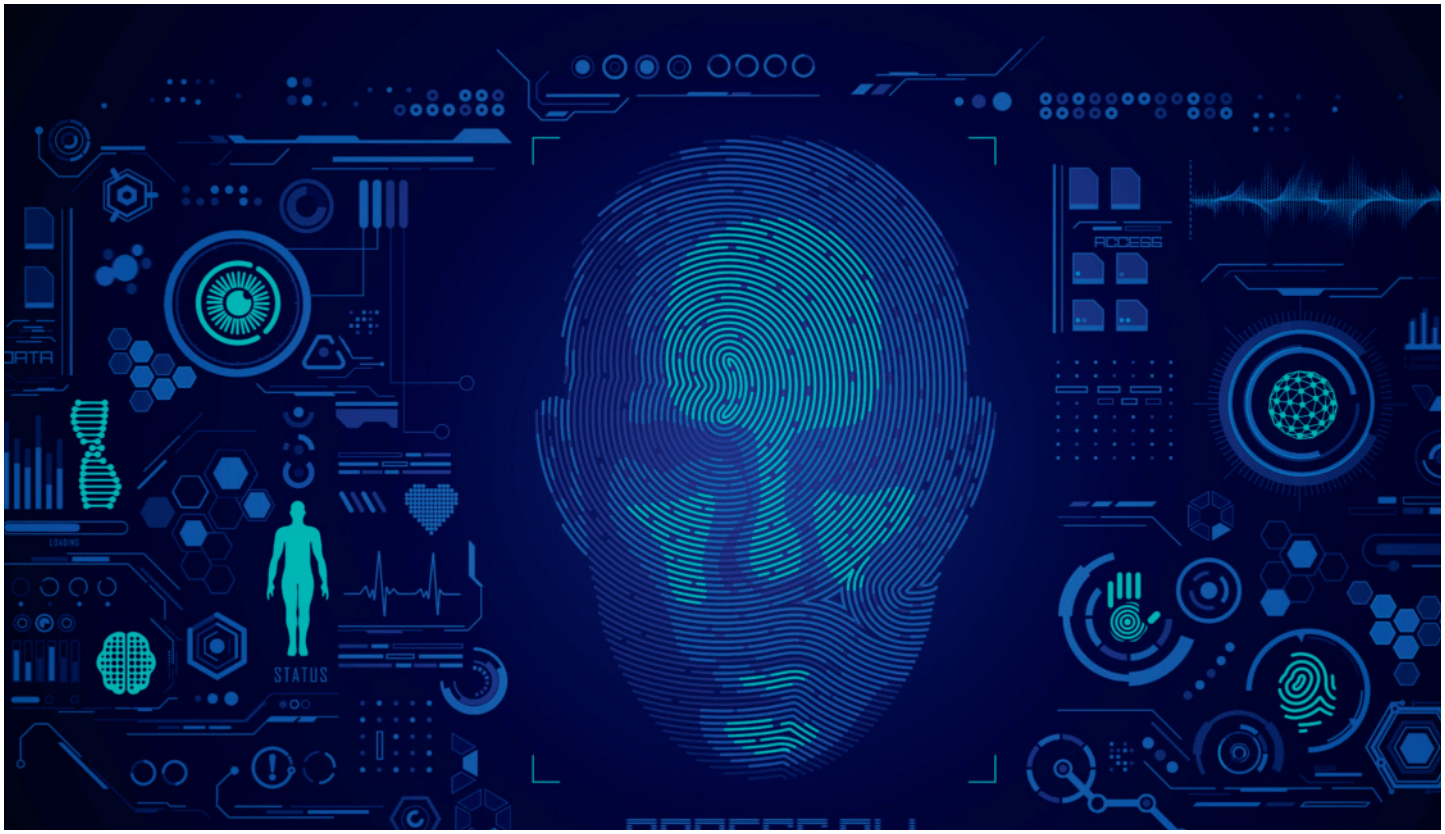
A key issue centered on whether, if BIPA had been violated, could plaintiff Cothron claim an actionable violation for each time her fingerprint scan was collected, captured, or disclosed to a third party – which may be thousands of times – or just the one time when her fingerprint scan was initially collected. All parties saw this as a question of great magnitude.

On appeal to the United States Court of Appeals for the Seventh Circuit, following removal to federal court from the Circuit Court of Cook County, the Seventh Circuit certified the following question to the Illinois Supreme Court:

> Do section 15(b) and 15(d) claims 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?" *Cothron v. White Castle System, Inc.,* 20 F.4th 1156, 1167 (7th Cir. 2021).

The case attracted substantial public interest in Illinois and around the country, and the court accepted many briefs amicus curiae. Briefs supporting White Castle were submitted by the Illinois Chamber of Commerce, Chamber of Commerce of the United States, Retail Litigation Center, Restaurant Law Center, National Retail Federation, Illinois Manufacturers' Association, National Association of Manufacturers, Illinois Health and Hospital Association, Illinois Retail Merchants Association, Chemical Industry Council of Illinois, Illinois Trucking Association, Mid-West Truckers Association, and Chicagoland Chamber of Commerce. Briefs supporting the plaintiff's position were submitted by the American Association for Justice, Employment Law Clinic of the University of Chicago Law School's Edwin F. Mandell Legal Aid Clinic, NELA/Illinois National Employment Law Project, Raise the Floor Alliance, and Electronic Privacy Information Center (EPIC).

The Illinois Supreme Court held that a separate claim accrues under the Act "each time a private entity scans or transmits an individual's biometric identifier or information in violation of section 15(b) or 15(d)." Pg. 2. The court's opinion and its dissent both viewed the matter as a direct interpretation of the statute's



plain language.

White Castle and *amici* argued that a violation of BIPA is like a tort loss of privacy. Damages in those cases presume a single injury at the event of publication and not recurrent injury with subsequent publications. This concept of injury demonstrates that the legislature intended to allow an actionable injury solely for the initial scan or transmission – the event of loss. The majority characterized these arguments as "nontextual" absent any reference to express language in the Act.

White Castle and *amici* also argued that construing the Act to allow multiple or repeated acts by one individual might result in "astronomical" damage awards and "annihilative liability" not contemplated by the legislature. White Castle stated that it had some 9,500 employees. Class-wide damages could reach $17 billion. Pg. 13. The court noted that regulatory statutes sometimes impose substantial liability.

"Each Time" Approach and Possibility of Significant Damages

The court's prior rulings on BIPA recognize the potential for significant damage awards. Pg. 14, citing *Rosenbach,* 2019 IL 123186, *McDonald*, 2022 IL 126511. Consumer protection and regulatory statutes often intend to deter conduct by imposing costs. As the Seventh Circuit had said in an early stage of the case, "private entities would have little incentive to course correct and comply if subsequent violations carry no legal consequences." *Cothron,* 20 F.4th at 1165.

The court answered the certified question in the affirmative. Each act of collection or dissemination may be an actionable violation of the Act. Pg. 13. The court offered two additional considerations.

At Paragraph 42, the court reiterated an important consideration in a class action proceeding in the relationship between a statutory violation and the calculation of damages. A trial court presiding over a class action has the discretion to fashion a damage award that (1) fairly compensates claiming class members; and (2) includes an amount designed to deter future violations, without destroying a defendant's business. The court noted that "there is no language in the Act suggesting legislative intent to authorize a damages award that would result in the financial destruction of a business." *Pg.* 14, ¶ 42.

In a dissent, Justice Overstreet, joined by Chief Justice Theis and Justice Holder White, disagreed with the majority's interpretation of the statutory language. Pg. 15. If the plaintiff was injured at all by the biometric data collection, she was only injured by the initial collection. The dissent stated that "there is only one loss of control or privacy, and this happens when the information is first obtained." Pg. 18, emphasis in original.

In further dissent upon denial of rehearing, the same Justices stated that, at minimum, the court should clarify and provide guidance to lower courts regarding the imposition of damages under the Act – including its instructions on a trial court's discretion to fashion damages that fairly compensate for injury and deter future violations without destroying defendant's business. *Pg.* 18.

Pending BIPA Cases

Observers are closely watching pending BIPA cases, including *Roger v. BNSF,* N.D. Ill. 19 C 3038. Plaintiff Rogers claims that he is a truck driver who drove to and from Defendant BNSF's railyards.

To enter these railyards, he was required to scan a biometric identifier into a device for an automated gate control system (AGS). That system was installed and operated by a third party, Remprex. The plaintiff proceeds on his claim and on behalf of "all individuals whose fingerprint information was registered using the AGS at one of BNSF's four Illinois facilities at any time between April 4, 2014, and January 25, 2020."

In October 2022, a jury found for the plaintiff class and awarded $228 million. On June 30, 2023, the trial court, Matthew F. Kennelly, District Judge, granted the defendant's motion for a new trial pursuant to Federal Rule of Civil Procedure 59 (a). The case is noteworthy with respect to the size of the verdict, the way it was calculated, and the District Court's order vacating the verdict and granting a new trial on damages.

Prior to trial, the court found that damages under BIPA could be awarded on a per-violation basis if the jury found intentional violations of the Act. The jury found that BNSF had recklessly or intentionally committed 445,600 violations. Applying the "each time" violation approach, as *Cothron* calls it, resulted in a substantial verdict, calculated as follows: the statute states $5,000 per violation; multiplying $5,000 x45,600 = $228,000,000. By that arithmetic, they reached a verdict of $228 million.

The District Court examined the evidence presented at trial and an extensive discussion of *Cothron* and Federal Court application of the Illinois Supreme Court's interpretation of Illinois law. The memorandum opinion is valuable reading.

The District Court discussed its understanding of *Cothron's* reference to court discretion in rejecting "astronomical" damage awards or "annihilative liability" (Cothron ¶ 40-42). Although the Illinois Supreme Court discussed the *court's* discretion because class actions are a creature of equity in Illinois courts, it is a settled issue in federal court that "class action plaintiffs may obtain a jury trial on any legal issues they present," the court held, citing to *Ortiz v. Fibreboard Corp.,* 527 U.S. 815. The jury does not solely conduct an arithmetic calculation; it considers all aspects of the award including the discretion referenced in *Cothron.* On that basis, the court vacated the verdict and granted a new trial on the issues of damages only.

Business Implications of Changes in Laws and Technology

The Illinois General Assembly considered amendments to the Act in the 2023 Spring Session, but it did not pass a bill. News reports suggest future legislative efforts in Springfield or perhaps federal legislative action. Nonetheless, *White Castle* remains the law. It helps to understand the court's decision and its underlying landscape.

It is safe to conclude that while regulation on collecting, storing, and disseminating biometric data may be changing, it will include the potential of significant damages for unauthorized collection or dissemination. Meanwhile, technological innovations and market use for such data are changing even faster.

A divided Illinois Supreme Court has given its opinion. A class action is a creature of equity, even when the nature of the claim is a violation of a dynamic statute, *Cothron* reiterates. Although the cause of action is statutory, it regards the common law interest of privacy, and a jury decides the ultimate questions of fact, including damages.

BIPA claims can be made on each unauthorized act of collection and each dissemination of biometric data, which can result in substantial liability. Astute counsel to any business that collects, stores, or receives biometric data should be aware of what is changing in biometric privacy regulation. ■

Judge James E. Snyder (ret.) served as a Judge of the Circuit Court of Cook County for 16 years, received the CBA/CBF John Paul Stevens Award in 2022, and is now a mediator/arbitrator and special master with JAMS.