Illinois Official Reports

Appellate Court

Mora v. J&M Plating, Inc., 2022 IL App (2d) 210692

Appellate Court Caption	TRINIDAD MORA, Individually and on Behalf of All Individuals Similarly Situated, Plaintiff-Appellant, v. J&M PLATING, INC., Defendant-Appellee.
District & No.	Second District No. 2-21-0692
Filed	November 30, 2022
Decision Under Review	Appeal from the Circuit Court of Winnebago County, No. 21-CH-22; the Hon. Donna R. Honzel, Judge, presiding.
Judgment	Reversed and remanded.
Counsel on Appeal	Carl V. Malmstrom, of Wolf Haldenstein Adler Freeman & Herz LLC, of Chicago, and Max S. Roberts (*pro hac vice*), of Bursor & Fisher, P.A., of New York, New York, for appellant. Joshua G. Vincent, Michael F. Iasparro, and Stephen D. Mehr, of Hinshaw & Culbertson LLP, of Chicago, for appellee.

Panel JUSTICE JORGENSEN delivered the judgment of the court, with opinion.
Presiding Justice Brennan and Justice Schostok concurred in the judgment and opinion.

OPINION

¶ 1 Plaintiff, Trinidad Mora, sued defendant, J&M Plating, Inc., asserting that defendant violated the Biometric Information Privacy Act (Biometric Act) (740 ILCS 14/1 *et seq.* (West 2020)) by failing to establish a retention-and-destruction schedule for the possession of biometric identifiers and biometric information (collectively, biometric data) until four years after it first possessed plaintiff's biometric data. *Id.* § 15(a). The trial court granted defendant's motion for summary judgment (735 ILCS 5/2-1005(c) (West 2020)), finding that section 15(a) of the Biometric Act established no time limits by which a private entity must establish a retention-and-destruction schedule for biometric data. Plaintiff appeals. We reverse and remand.

¶ 2 I. BACKGROUND

¶ 3 A. The Biometric Act

¶ 4 The Biometric Act, enacted in 2008,[1] regulates " 'the collection, use, safeguarding, handling, storage, retention, and destruction of biometric identifiers and information.' " *Rosenbach v. Six Flags Entertainment Corp.*, 2019 IL 123186, ¶ 19 (quoting 740 ILCS 14/5(g) (West 2016)). The Biometric Act defines a "biometric identifier" as a "retina or iris scan, fingerprint, voiceprint, or scan of hand or face geometry." 740 ILCS 14/10 (West 2020). "Biometric information" means "any information, regardless of how it is captured, converted, stored, or shared, based on an individual's biometric identifier used to identify an individual." *Id.* The legislature, through the Biometric Act, "codified that individuals possess a right to privacy in and control over their biometric identifiers and biometric information." *Rosenbach*, 2019 IL 123186, ¶ 33.

¶ 5 Under the Biometric Act:

> "any person 'aggrieved' by a violation of its provisions 'shall have a right of action *** against an offending party' and 'may recover for each violation' the greater of liquidated damages or actual damages, reasonable attorney fees and costs, and any other relief, including an injunction, that the court deems appropriate." *Id.* ¶ 1 (quoting 740 ILCS 14/20 (West 2016)).

¶ 6 The Biometric Act "vests in individuals and customers the right to control their biometric information by requiring notice before collection and giving them the power to say no by withholding consent." *Id.* ¶ 34. Section 15 of the Biometric Act "imposes on private entities *** various obligations regarding the collection, retention, disclosure, and destruction of" biometric data. *Id.* ¶ 20. These obligations include the following.

[1]The Biometric Act took effect upon becoming law. 740 ILCS 14/99 (West 2020).

¶ 7 Section 15(a) of the Biometric Act, which is at issue in this case, contains a requirement to develop, publish, and comply with a retention-and-destruction schedule. It provides:

> "A private entity in possession of biometric identifiers or biometric information must develop a written policy, made available to the public, establishing a retention schedule and guidelines for permanently destroying biometric identifiers and biometric information when the initial purpose for collecting or obtaining such identifiers or information has been satisfied or within 3 years of the individual's last interaction with the private entity, whichever occurs first. Absent a valid warrant or subpoena issued by a court of competent jurisdiction, a private entity in possession of biometric identifiers or biometric information must comply with its established retention schedule and destruction guidelines." 740 ILCS 14/15(a) (West 2020).

¶ 8 Section 15(b) contains the following notice requirement:

> "(b) No private entity may collect, capture, purchase, receive through trade, or otherwise obtain a person's or a customer's biometric identifier or biometric information, unless it first:
>
> (1) informs the subject or the subject's legally authorized representative in writing that a biometric identifier or biometric information is being collected or stored;
>
> (2) informs the subject or the subject's legally authorized representative in writing of the specific purpose and length of term for which a biometric identifier or biometric information is being collected, stored, and used; and
>
> (3) receives a written release executed by the subject of the biometric identifier or biometric information or the subject's legally authorized representative." *Id.* § 15(b).

¶ 9 Section 15(c) prohibits profiting from a transaction involving a person's or a customer's biometric data. *Id.* § 15(c) ("No private entity in possession of a biometric identifier or biometric information may sell, lease, trade, or otherwise profit from a person's or a customer's biometric identifier or biometric information."). Section 15(d) prohibits the disclosure or redisclosure of a person's or customer's biometric data, unless the subject consents or the disclosure is required in certain circumstances. See *id.* § 15(d). Finally, section 15(e) requires a private entity in possession of biometric data to store, transmit, and protect it (1) using the reasonable standard of care in its industry and (2) in a manner as or more protective than the manner in which it stores, transmits, and protects other confidential and sensitive information. See *id.* § 15(e).

¶ 10 These provisions are enforceable through private rights of action. *Rosenbach*, 2019 IL 123186, ¶ 21. Section 20 of the Biometric Act provides that "[a]ny person aggrieved by a violation of this Act shall have a right of action in a State circuit court or as a supplemental claim in federal district court against an offending party." 740 ILCS 14/20 (West 2020). Section 20 further provides that

> "[a] prevailing party may recover for each violation:
>
> (1) against a private entity that negligently violates a provision of this Act, liquidated damages of $1,000 or actual damages, whichever is greater;
>
> (2) against a private entity that intentionally or recklessly violates a provision of this Act, liquidated damages of $5,000 or actual damages, whichever is greater;

(3) reasonable attorneys' fees and costs, including expert witness fees and other litigation expenses; and

(4) other relief, including an injunction, as the State or federal court may deem appropriate." *Id.*

¶ 11 When a private entity fails to comply with one of section 15's requirements, that violation constitutes an invasion, impairment, or denial of the statutory rights of any person or customer whose biometric data is subject to breach. *Rosenbach*, 2019 IL 123186, ¶ 33. "The violation, in itself, is sufficient to support the individual's or customer's statutory cause of action." *Id.* "Other than the private right of action authorized in section 20 of [the Biometric Act], no other enforcement mechanism is available." *Id.* ¶ 37. The legislature has imposed safeguards to ensure that privacy rights in biometric data "are properly protected before they can be compromised and by subjecting private entities who fail to follow the statute's requirements to substantial potential liability (740 ILCS 14/20 (West 2016)) whether or not actual damages, beyond violation of the law's provisions, can be shown." *McDonald v. Symphony Bronzeville Park, LLC*, 2022 IL 126511, ¶ 48. Finally, the workers' compensation statute's exclusivity provision does not bar Biometric Act claims. *Id.* ¶ 50 ("[b]ecause the injury alleged is not the type of injury compensable in a workers' compensation proceeding, [the plaintiff's] lawsuit is not preempted by the exclusive-remedy provisions of the [statute]").

¶ 12 B. Plaintiff's Complaint

¶ 13 Plaintiff began working for defendant on July 2, 2014, and began clocking into his job via fingerprint scan in September 2014. In May 2018, defendant established a written retention-and-destruction schedule for biometric data, and, on May 22, 2018, plaintiff signed defendant's policy[2] and consented to the collection and use of his biometric data. Plaintiff's employment was terminated on January 7, 2021, and pursuant to defendant's retention-and-destruction schedule, plaintiff's biometric information was destroyed approximately two weeks after his termination.

¶ 14 On February 16, 2021, plaintiff filed a class-action complaint (735 ILCS 5/2-801 (West 2020))[3] against defendant, alleging violations of section 15(a) and 15(b) of the Biometric Act. Plaintiff asserted that defendant required employees to "clock in" with their fingerprints and that defendant collected, stored, and used employee fingerprints and associated personally identifying information without first providing notice, obtaining informed consent, or, as relevant to this appeal, publishing a data retention-and-destruction schedule.

¶ 15 In count I, plaintiff sought declaratory and injunctive relief and damages for defendant's alleged violation of section 15(a) (failure to institute, maintain, and adhere to publicly available retention schedule). In count II, plaintiff sought damages for alleged violations of section 15(b) (failure to obtain informed written consent and release before obtaining biometric data).

---

[2] Defendant's two-page policy, titled the "J&M PLATING BIOMETRIC INFORMATION PRIVACY POLICY," contains both its section 15(b) notice and its section 15(a) retention-and-destruction schedule, the latter of which provides that "[a]n employee's biometric information will be destroyed upon termination of the employment relationship or if biometric information is no longer needed."

[3] Plaintiff defined the class as "[a]ll individuals who had their fingerprints collected, captured, received[,] or otherwise obtained and/or stored by [d]efendant in the state of Illinois."

Plaintiff argued that defendant invaded his statutorily protected right to privacy in his biometric data, never adequately informed him or the class of its biometric collection practices, never obtained the requisite written consent from plaintiff or the class regarding plaintiff's practices, and never provided to them any retention-and-destruction schedule.

¶ 16 On April 28, 2021, defendant moved to dismiss plaintiff's complaint (*id.* §2-619(a)(5), (9)), asserting that it instituted a biometric information privacy policy, plaintiff signed defendant's policy, he consented to the collection and use of his biometric data, his employment was terminated, and, pursuant to defendant's written retention-and-destruction schedule, his biometric data was destroyed upon his termination. Thus, count I was defeated because plaintiff's information was destroyed upon his termination, the statute of limitations barred plaintiff's section 15(b) claim (count II), and his claim was barred by the Workers' Compensation Act (820 ILCS 305/1 *et seq.* (West 2020)). Defendant attached to its motion an affidavit from Martina Schumaker, its chief financial officer. Schumaker averred that plaintiff was defendant's employee from July 2, 2014, through January 7, 2021. In September 2014, defendant began utilizing a fingerprint scan system for timekeeping purposes and collected images of employees' fingerprints for such purposes that month. It developed and publicized its Biometric Act policy in May 2018, which was published at in-person meetings on May 20 and 22, 2018. On May 22, 2018, by signing a copy of the policy, plaintiff acknowledged receipt of the policy and consented to defendant's collection and use of his biometric data for timekeeping purposes. Plaintiff's last day of employment with defendant was January 7, 2021, and his biometric data that was collected for timekeeping purposes was destroyed upon his termination.

¶ 17 On July 14, 2021, the trial court dismissed count II of plaintiff's complaint, finding that the cause of action under section 15(b) of the Biometric Act accrued in September 2014 and that a five-year limitations period applied. Thus, the claim was time-barred. As to count I, the section 15(a) claim at issue in this appeal, the court denied defendant's motion to dismiss. It determined that defendant's motion raised fact-based arguments properly resolved in a summary-judgment motion.

¶ 18 C. Defendant's Summary-Judgment Motion

¶ 19 On September 30, 2021, defendant moved for summary judgment on count I of plaintiff's complaint, arguing that plaintiff's biometric data was destroyed two weeks after his last day of work and, thus, he could not establish a violation of section 15(a) of the Biometric Act. It asserted that section 15(a) did not have any timing language for the establishment of a retention-and-destruction schedule and, therefore, it was of no import that defendant's policy was not in place *before* plaintiff's biometric data was first obtained. Defendant attached an affidavit from Albert Cloherty, "manager II-tech support" with ADP, Inc., defendant's vendor. Cloherty averred that he reviewed ADP's records and that they reflected that any biometric information ADP possessed relating to plaintiff that was generated by time clocks or time clock attachments during plaintiff's employment with defendant was destroyed on or about January 21, 2021.

¶ 20 Plaintiff responded that defendant waited nearly four years after it began possessing biometric data to establish a retention-and-destruction schedule and that this did not comply with the statute. Further, defendant's retroactive compliance did not cure its earlier violations, because plaintiff's biometric data was already exposed to the harm the legislature sought to

prevent. Plaintiff argued that section 15(a) must be read to require an entity to establish a retention-and-destruction schedule *prior to* possessing an individual's biometric data. Alternatively, plaintiff argued that defendant was required to establish a schedule *the moment it first possessed* plaintiff's biometric data, not years later.

¶ 21 The trial court granted defendant's motion, finding that the statute contains no timing language and "is written as if the private entity is already in possession of biometric identifiers and information." The court determined that defendant had a retention-and-destruction schedule, that it obtained plaintiff's consent, and that plaintiff's data was destroyed shortly after his employment was terminated. Thus, "there's no harm here. They ultimately did comply. There is no timing language in the statute." Plaintiff appeals.

¶ 22 II. ANALYSIS

¶ 23 Plaintiff argues that the trial court erred in granting defendant summary judgment on his section 15(a) claim, because the Biometric Act required defendant to establish a retention-and-destruction schedule for biometric data *prior to* its possession of such data or, alternatively, *at the moment of possession or within a reasonable time thereafter*. Defendant's establishment of a schedule four years after the fact (*i.e.*, after defendant began collecting plaintiff's biometric data), plaintiff asserts, did not comply with the Biometric Act, and any contrary conclusion strips the statute of any enforceability. For the following reasons, we agree that the trial court erred in granting defendant summary judgment and conclude that the Biometric Act requires a private entity such as defendant to *develop* a retention-and-destruction schedule upon *possession* of biometric data. Defendant's establishment of a retention-and-destruction schedule four years after it first possessed such data for plaintiff violated section 15(a).

¶ 24 Preliminarily, we note that defendant argues that plaintiff's statement of facts contains no citations of the record on appeal and is argumentative, in violation of Illinois Supreme Court Rule 341(h)(6) (eff. Oct. 1, 2020). Rule 341(h)(6) requires an appellant's brief to contain a "[s]tatement of facts, which shall contain the facts necessary to an understanding of the case, stated accurately and fairly without argument or comment, and with appropriate references to the pages of the record on appeal." *Id.* The rules of procedure regarding appellate briefs are not mere suggestions, and when procedural violations interfere with our review of the issues on appeal, it is within our discretion to, *inter alia*, strike the brief for failure to comply with the rules. See *Parkway Bank & Trust Co. v. Korzen*, 2013 IL App (1st) 130380, ¶ 10. Nevertheless, where, as here, violations of supreme court rules are not so flagrant as to hinder or preclude our review and where defendant has provided a statement of facts, we will disregard any noncompliant statements in plaintiff's brief. See *In re Marriage of Wendy S.*, 2020 IL App (1st) 191661, ¶ 15; see also *Twardowski v. Holiday Hospitality Franchising, Inc.*, 321 Ill. App. 3d 509, 511 (2001) (we may review an otherwise insufficient appeal where "we understand the issue plaintiff intends to raise and especially where the court has the benefit of a cogent brief of the other party").

¶ 25 Turning to the merits, a trial court may grant summary judgment only "if the pleadings, depositions, and admissions on file, together with the affidavits, if any, show that there is no genuine issue as to any material fact and that the moving party is entitled to a judgment as a matter of law." 735 ILCS 5/2-1005(c) (West 2020). The trial court considers the documents and exhibits in the light most favorable to the nonmoving party. *Home Insurance Co. v. Cincinnati Insurance Co.*, 213 Ill. 2d 307, 315 (2004).

¶ 26 "Summary judgment is a drastic measure and should only be granted if the movant's right to judgment is clear and free from doubt." *Outboard Marine Corp. v. Liberty Mutual Insurance Co.*, 154 Ill. 2d 90, 102 (1992). However, "[m]ere speculation, conjecture, or guess is insufficient to withstand summary judgment." *Sorce v. Naperville Jeep Eagle, Inc.*, 309 Ill. App. 3d 313, 328 (1999). " 'The purpose of summary judgment is not to try an issue of fact but *** to determine whether a triable issue of fact exists.' " *Schrager v. North Community Bank*, 328 Ill. App. 3d 696, 708 (2002) (quoting *Luu v. Kim*, 323 Ill. App. 3d 946, 952 (2001)).

¶ 27 The issue in this case involves a statutory construction question, which constitutes a question of law and is thus appropriate for summary judgment. *Hooker v. Retirement Board of the Firemen's Annuity & Benefit Fund of Chicago*, 2013 IL 114811, ¶ 15. We review *de novo* issues involving statutory construction and summary-judgment rulings. *Id.*

¶ 28 "Our primary objective when construing a statute is to ascertain and give effect to the intent of the legislature." *Eighner v. Tiernan*, 2021 IL 126101, ¶ 19. "The most reliable indicator of legislative intent is the plain and ordinary meaning of the statutory language." *Id.* "When construing statutory language, we view [a] statute in its entirety, construing words and phrases in light of other relevant statutory provisions and not in isolation." *Id.*

¶ 29 "When the statutory language is plain and unambiguous, we may not depart from the law's terms by reading into it exceptions, limitations, or conditions the legislature did not express, nor may we add provisions not found in the law." *Rosenbach*, 2019 IL 123186, ¶ 24. Nevertheless, in construing a statute, a court may consider the reason for the law, the problems sought to be remedied, the purposes to be achieved, and the consequences of construing the statute one way or another. *Hubble v. Bi-State Development Agency of the Illinois-Missouri Metropolitan District*, 238 Ill. 2d 262, 268 (2010).

¶ 30 Plaintiff argues that section 15(a) of the Biometric Act reflects the legislature's intent that a retention-and-destruction schedule be established prior to the possession of biometric data (or, alternatively, at the moment of possession or within a reasonable time thereafter).[4] Plaintiff notes that the General Assembly stated that "[b]iometrics are unlike other unique identifiers that are used to access finances and other sensitive information. *** Biometrics *** are biologically unique to the individual; therefore, once compromised, the individual has no recourse, is at heightened risk for identity theft, and is likely to withdraw from biometric-facilitated transactions." 740 ILCS 14/5(c) (West 2020). Further, it stated that "[t]he full ramifications of biometric technology are not fully known." *Id.* § 15(f). Plaintiff contends that no other provision of the Biometric Act allows for retroactive compliance and that allowing retroactive compliance with section 15(a) would undermine the statute's legislative purpose of empowering individuals with biometric privacy rights *before* such rights are violated.

---

[4]In *Bernal v. ADP, LLC*, No. 2017-CH-12364, 2019 WL 5028609 (Cir. Ct. Cook County, Aug. 23, 2019), which plaintiff cites, the trial court granted the defendant biometric technology provider's motion to dismiss (735 ILCS 5/2-615 (West 2018)), without prejudice, the plaintiff employee's section 15(a) Biometric Act claim. The plaintiff had alleged the defendant had not established a policy prior to taking the plaintiff's biometric data. The trial court found that section 15(a) does not explicitly require that the schedule exist *prior* to possession of the biometric data. *Bernal*, 2019 WL 5028609, at *2. However, the court also determined that the plaintiff's allegation "does not exclude the possibility that [the] [d]efendant made available to the public an established schedule and guidelines *when*, and not before, it was in possession of [the] Plaintiff's biometric information." (Emphasis added.) *Id.* Thus, the complaint, the court determined, failed to state a claim. *Id.*

¶ 31 Plaintiff also asserts that it is not relevant whether an entity that did not have a retention-and-destruction schedule in place upon the statute's effective date would be in automatic violation of the statute and be subject to statutory penalties for conduct that was not prohibited at the time it took place. In plaintiff's view, by 2014, when defendant first possessed plaintiff's biometric data, entities such as defendant had already had six years from the statute's enactment to implement procedures that would allow them to comply with the Biometric Act. By 2018, plaintiff notes, when defendant did finally implement its schedule, an additional four years had elapsed for defendant to comply. Thus, plaintiff reasons, even if entities had not been capable of immediate compliance when the statute was enacted, waiting 6 or 10 years is an unreasonable time to attain compliance.

¶ 32 Plaintiff also contends that allowing private entities unlimited time to comply with section 15(a), as the trial court did, would lead to absurd results and undermine both the enforceability of the statute and the legislature's objective of protecting biometric data from problems before they occur. For example, plaintiff posits that a private entity could wait until a data breach has exposed all biometric data before establishing a retention-and-destruction schedule and still comply with section 15(a). Or, plaintiff suggests, a private entity could choose to never comply for decades, so long as, when someone eventually brought up the deficiency, the private entity eventually established a schedule. Plaintiff argues that common sense dictates that there is not an unlimited time to comply with the statute and that such an understanding of section 15(a) would eliminate the incentive for compliance with the statutory damages provision. See *Rosenbach*, 2019 IL 123186, ¶ 37 ("[t]o require individuals to wait until they have sustained some compensable injury beyond violation of their statutory rights before they may seek recourse *** would be completely antithetical to [the Biometric Act's] preventative and deterrent purposes").

¶ 33 Defendant responds that section 15(a) is concerned with the timely destruction of biometric data when it is no longer needed and requires a private entity that possesses such data to have a policy in place that ensures the data will be destroyed when the purpose for which it was collected has ended or within three years after the parties' last interaction, whichever occurs first. There is no need, it asserts, for this court to rewrite the statute and provide a schedule or timetable within which an entity must publish or adopt its schedule. The temporal component of section 15(a) is, according to defendant, self-evident, and the statutory duty is satisfied so long as a schedule exists *on the day the biometric data possessed by a defendant is no longer needed or the parties' relationship has ended*. It argues that section 15(a)'s purpose is to ensure the data destruction policy *exists* when either the data is no longer needed or the parties' relationship has ended, whichever occurs first, and not *before* the earlier of these occurrences. No other duty is imposed by section 15(a), defendant contends. Defendant also argues that, had the legislature intended to impose a duty to have a schedule in place before or at the moment an entity collects biometric data, it could have easily written section 15(a) to say that such a schedule must be adopted prior to and upon collecting the data (or within a reasonable time thereafter). It notes that, in contrast, section 15(b) contains a temporal requirement for compliance.

¶ 34 It is undisputed, defendant notes, that it had a policy in place when plaintiff's relationship with defendant ended, and plaintiff's biometric data was destroyed within two weeks after his employment with defendant ended. Defendant argues that section 15(b) of the Biometric Act, which establishes a notice-and-consent requirement, grants a person like plaintiff the ability to

make an informed decision about whether to disclose his or her biometric data. Thus, the interest served is a person's right to control his or her private data. Plaintiff's argument that he was entitled to know how long defendant would store his data was the subject of his section 15(b) claim, which was dismissed with prejudice and from which plaintiff did not appeal. Defendant contends that plaintiff cannot resurrect his dismissed claim by bootstrapping section 15(b) protections to a section 15(a) claim.

¶ 35 Defendant also argues that the Biometric Act's organizational structure regulates different steps in the process as they occur, with section 15(b) addressing the initial collection of data. Storage and use are governed by sections 15(c), 15(d), and 15(e), and retention and destruction are governed by section 15(a). Viewed as a whole, defendant asserts, the duty imposed by section 15(a) is plainly tied to when either the data is no longer needed or the parties' relationship has ended.

¶ 36 Defendant disagrees with plaintiff's argument that, under the trial court's reasoning, a suit could not be brought until an injury has resulted from a defendant's failure to have a schedule in place and that this defeats the statute's preventative and deterrent purposes. Defendant contends that this is a strawman argument that we need not reach here, because defendant had a schedule in place when the circumstances contemplated by section 15(a) arose. Further, defendant notes that there is no evidence that plaintiff's data was ever compromised due to the absence of a policy. Plaintiff's fear, it suggests, is entirely hypothetical. Defendant also maintains that plaintiff's argument transforms the Biometric Act, which is a fault-based statute, into a strict liability regime under which liability would attach as soon as a defendant came into possession of biometric data. The statutory language, it argues, does not support such a construction.

¶ 37 We conclude that the trial court erred in granting defendant summary judgment. Section 15(a) of the Biometric Act provides:

> "A private entity *in possession of* biometric identifiers or biometric information *must develop a written policy*, made available to the public, establishing a retention schedule and guidelines for permanently destroying biometric identifiers and biometric information when the initial purpose for collecting or obtaining such identifiers or information has been satisfied or within 3 years of the individual's last interaction with the private entity, whichever occurs first. Absent a valid warrant or subpoena issued by a court of competent jurisdiction, a private entity in possession of biometric identifiers or biometric information must comply with its established retention schedule and destruction guidelines." (Emphases added.) 740 ILCS 14/15(a) (West 2020).

¶ 38 Thus, section 15(a) specifies that a private entity "in possession of" biometric data "must" (1) "develop a written policy," (2) publish it, and (3) comply with it. The policy must contain (1) "a retention schedule" and (2) "guidelines for permanently destroying" biometric data "when the initial purpose for collecting or obtaining such" data "has been satisfied or within 3 years of the individual's last interaction with the private entity, whichever occurs first." *Id.* The explicit trigger for the *development* of the written policy (*i.e.*, the retention-and-destruction schedule) is the private entity's *possession*[5] of biometric data. *Id.*

---

[5]" 'Possession' means 'the act or condition of having in or taking into one's control or holding at one's disposal.' Webster's Third New International Dictionary 1770 (1986); see also Black's Law Dictionary 1201 (8th ed. 2004) (listing the primary definition of 'possession' as '[t]he fact of having or

¶ 39 Our conclusion is consistent with the statutory scheme, which imposes upon private entities the obligation to establish Biometric-Act-compliant procedures to protect employees' and customers' biometric data. Section 15(b) of the Biometric Act provides that a private entity may not collect, capture, purchase, or trade biometric data, unless it first (1) provides written notice to the subject that it is collecting or storing the subject's data and the specific purpose and length of time for which it is being collected, etc., and (2) receives a written release by the subject of the data. *Id.* § 15(b). Our reading of section 15(a) is consistent with section 15(b)'s requirement that, prior to the time a private entity collects, captures, purchases, or otherwise obtains a subject's biometric data, it must first inform the subject of the "length of term for which [biometric data] is being collected, stored, and used." *Id.* § 15(b)(2). We can discern no rational reason for the legislature to have intended that a private entity "develop" a "retention schedule and guidelines for permanently destroying" (*id.* § 15(a)) biometric data at a *different* time from that specified in the notice requirement in section 15(b), which itself must inform the subject of the length of time for which the data will be stored (*i.e.*, retained), etc. For this reason, we also conclude that the duty to develop a schedule upon possession of the data necessarily means that the schedule must exist on that date, not afterwards. This is consistent, we believe, with the Biometric Act's preventative and deterrent purposes (*Rosenbach*, 2019 IL 123186, ¶ 37) and is the only reasonable interpretation of the language of section 15(a). See *Hartney Fuel Oil Co. v. Hamer*, 2013 IL 115130, ¶ 25 ("[s]tatutory provisions should be read in concert and harmonized"); see also *Eighner*, 2021 IL 126101, ¶ 19 ("[w]hen construing statutory language, we view [a] statute in its entirety, construing words and phrases in light of other relevant statutory provisions and not in isolation").

¶ 40 We reject defendant's argument that the statutory duty is satisfied so long as a schedule exists on the day that the biometric data possessed by a defendant is no longer needed or the parties' relationship has ended. The statutory language belies this interpretation, because it explicitly requires an entity "in possession of" the data to "develop" and publish its retention-and-destruction schedule. 740 ILCS 14/15(a) (West 2020). It does *not* state that the schedule must be in place upon the earlier of the two specified conditions—when the collection purpose is satisfied or within three years of the last interaction, whichever occurs first. Rather, again, the statute provides that an "entity in possession of biometric [data] must develop a written policy." *Id.* The duty to develop a schedule is triggered by possession of the biometric data. The two specified conditions are referenced for purposes of the retention schedule and are deadlines for the permanent destruction of the biometric data in the private entity's possession. We also reject defendant's assertion that plaintiff's argument that he was entitled to know how long defendant would store his data was the subject of his section 15(b) claim and that plaintiff cannot resurrect his dismissed claim by bootstrapping section 15(b) protections to a section 15(a) claim. This argument ignores the clear language of section 15(a), which requires a private entity, upon possession of biometric data, to develop and make public a written retention-and-destruction schedule. Although the statute must be read as a whole (*Eighner*, 2021 IL 126101, ¶ 19), a private entity's obligations under section 15(b) (specifically, to first provide written notice that biometric data is being collected or stored, the purpose for which it is being

---

holding property in one's power; the exercise of dominion over property'). Thus, 'possession,' as ordinarily understood, occurs when a person has or takes control of the subject property or holds the property at his or her disposal." *People v. Ward*, 215 Ill. 2d 317, 325 (2005). The scanning and collection or storing of fingerprint data clearly involves the taking of property and meets this definition.

collected or stored, and the length of time for which it is being collected or stored and to obtain consent to the collection of the data before it is collected or stored) are separate and distinct from those under section 15(a), and the sections serve different purposes. Section 15(a)'s purpose is (1) to notify the public (including any individual whose biometric data is in a private entity's possession) that the entity has a retention schedule that provides that the data will be kept/stored for only a finite time and reflects the deadline for the data's destruction and (2) to require the entity to comply with the schedule. This is distinct from section 15(b)'s purpose, which is to provide individuals certain information when a private entity seeks to obtain their biometric data (including the length of term for which the data will be stored) and to give them control over whether to allow their data to be collected.

¶ 41 The trial court erred in finding that, because plaintiff sustained "no harm," there could not be a violation of the Biometric Act. This is contrary to the supreme court's interpretation of the statute. In *Rosenbach*, the supreme court held that "a person need not have sustained actual damage beyond violation of his or her rights under [the Biometric Act] in order to bring an action under it"; that is, "[t]he violation, in itself, is sufficient to support the individual's or customer's statutory cause of action." *Rosenbach*, 2019 IL 123186, ¶¶ 28, 33.

¶ 42 Here, defendant began collecting plaintiff's biometric data in September 2014, and this triggered its obligation under section 15(a) to develop a retention-and-destruction schedule. Defendant did not have a schedule in place until May 2018, or nearly four years later. Thus, it violated section 15(a).

¶ 43 In summary, the trial court erred in granting defendant summary judgment.

¶ 44 III. CONCLUSION

¶ 45 For the reasons stated, we reverse the judgment of the circuit court of Winnebago County and remand the cause for further proceedings consistent with this decision.

¶ 46 Reversed and remanded.