Loyola University Chicago Law Journal

Volume 50
Issue 4 *Summer 2019*

Article 14

2019

The Litigation Rollercoaster of BIPA: A Comment on the Protection of Individuals from Violations of Biometric Information Privacy

Anna L. Metzger

The Litigation Rollercoaster of BIPA: A Comment on the Protection of Individuals from Violations of Biometric Information Privacy

*Anna L. Metzger**

As technology progresses, businesses are enacting new programs that utilize emerging technology. Biometric data is an example of a tech capability that is becoming more popular for businesses. Companies can use an individual's unique body data to monitor their employees, collect data, and enhance security and convenience for their customers. While this technology is impressive, it comes with privacy and security concerns. In 2008, Illinois enacted the Biometric Information Privacy Act (BIPA) to address these concerns. BIPA aims to protect individuals by setting strict guidelines for data collection by private entities. Individuals can file suit for violations of this statute, so long as they can show that they are an aggrieved party.

Since June 1, 2017, over two hundred class actions have been filed in Illinois alleging claims under BIPA. In 2017, Illinois's Second District Appellate Court heard an appeal from a ruling in Rosenbach v. Six Flags Entertainment Corp. *and set forth an important new interpretation of BIPA. The appellate court found that the plaintiff was not an aggrieved party as they did not assert actual harm from the violation of BIPA. In 2018, Illinois's First District Appellate Court disagreed with this holding, and in the case of* Sekura v. Krishna Schaumburg Tan, Inc.*, held that a statutory violation of BIPA created an aggrieved party. Also in 2018, the Illinois Supreme Court agreed to hear the appeal of* Rosenbach.

On January 25, 2019, the Illinois Supreme Court handed down its decision in Rosenbach v. Six Flags Entertainment Corp. *In a unanimous decision, the court held a person is "aggrieved" when there is a technical violation of BIPA; a showing of further harm is not necessary to bring a cause of action under the statute. This Comment will examine the* Rosenbach *decision and analyze its overall logic, application of Illinois's statute and case law, and appreciation for the intent of the Illinois legislature.*

Last, this Comment will assess the impact of the Illinois Supreme Court's decision on the future of biometric data collection and provide suggestions for future corporate compliance.

---

* JD Candidate, Loyola University Chicago School of Law, 2020.

INTRODUCTION

As technology progresses, businesses are implementing new programs that utilize emerging technology.[1] Biometric data is an example of a technological capability that is becoming increasingly popular for

1. *See* Adam Rogers, *Innovation Case Studies: How Companies Use Technology to Solidify a Competitive Advantage*, FORBES (Apr. 13, 2018, 7:00 AM), https://www.forbes.com/sites/forbestechcouncil/2018/04/13/innovation-case-studies-how-companies-use-technology-to-solidify-a-competitive-advantage/#7ff2a0f51410 ("It's become impossible to separate business strategy from technological innovation, so everyone from retailers to health care professionals are investing heavily in tech solutions to help them market, improve offerings and drive business."); *see also Small Business Technology Trends*, DELOITTE: PERSP. (2018), https://www2.deloitte.com/us/en/pages/technology-media-and-telecommunications/articles/connected-small-businesses.html ("Digital technology is driving many changes in consumer behavior and the business environment. . . . The use of digital tools can help small businesse[s] to improve their performance and respond to changes in the business and consumer landscape in an agile manner.").

businesses.[2] In Illinois, use of biometric data has revealed a unique intersection between business priorities, technological advancements, and the privacy rights of individuals.[3] The legal community is currently grappling with this balance of business interests and the protection of individuals.[4] This debate has manifested in the form of lawsuits brought under an Illinois statute concerning biometric data: the Biometric Information Privacy Act.[5]

Biometrics are physical characteristics, such as fingerprints, face, iris, and voice that can be used for automated recognition of an individual.[6] Technologies use these characteristics because they are unique to each individual and do not change over time.[7] Current technology allows biometric data to be collected, analyzed, and saved; a user of biometric technology enrolls into a system by providing her information, and this information is stored and later used to recognize that user.[8] Government agencies and businesses utilize this biometric information for a variety of

2. *See* Hannah Zimmerman, *The Data of You: Regulating Private Industry's Collection of Biometric Information*, 66 U. KAN. L. REV. 637, 639 (2018) ("According to a market research report by Application, Technology, Function, & Geography, 'the biometrics market is expected to reach $32.73 billion by 2022.'"); *see also* Niya T. McCray, *Sensitive to the Touch: The Evolution of U.S. Biometric Privacy Law*, FOR DEF., May 2018, at 77, 77 (2018) (explaining that an increasing amount of employers and businesses are using biometric data to streamline, prevent timekeeping fraud, and to strengthen operational security).

3. *See* McCray, *supra* note 2, at 78 (noting that although biometrics are helpful to companies and the use of biometric data is surging, there are "unanswerable questions" about the security of biometrics that are driving legislation and litigation in Illinois).

4. *See id.*; *see also* Kwabena A. Appenteng & Philip L. Gordon, *Recent Illinois Appellate Court Ruling Could End the Recent Flood of Class Action Lawsuits Against Employers Under Illinois' Biometric Information Privacy Act*, LITTLER (Jan. 9, 2018), https://www.littler.com/publication-press/publication/recent-illinois-appellate-court-ruling-could-end-recent-flood-class (describing a conflict between employers who use biometric data and their employees, who are debating privacy rights under BIPA).

5. *See* Charles N. Insler, *Understanding the Biometric Information Privacy Act Litigation Explosion*, ILL. B.J., Mar. 2018, at 34, 49 ("Recent months have seen an explosion in litigation under BIPA. With technology constantly evolving and advancing, particularly in the field of biometric information, BIPA will almost certainly be a topic of discussion and a source of litigation for years to come . . . ."); *see also*, *e.g.*, Ann H. MacDonald & Lauren S. Novak, *Illinois Biometric Lawsuits: An Early Roadmap for Biometric Litigation*, SCHIFF HARDIN (Apr. 3, 2018), https://www.schiffhardin.com/insights/publications/2018/illinois-biometric-lawsuits-an-early-roadmap-for-biometric-litigation.

6. *See Biometrics*, U.S. DEP'T HOMELAND SECURITY (Feb. 6, 2017), https://www.dhs.gov/biometrics [hereinafter *DHS Biometrics*] (defining biometrics); *see also* Dep't of Comput. Sci. & Eng'g, Biometrics Research Grp., *What Is Biometrics?*, MICH. ST. U., http://biometrics.cse.msu.edu/info/index.html (last visited June 16, 2019) [hereinafter *What Is Biometrics?*] (describing anatomical and behavioral characteristics that biometric recognition utilizes).

7. *See, e.g.*, *DHS Biometrics*, *supra* note 6; *What Is Biometrics?*, *supra* note 6.

8. *See, e.g.*, *What Is Biometrics?*, *supra* note 6; *see also* BIOMETRIC RECOGNITION: CHALLENGES AND OPPORTUNITIES 2 (Joseph N. Pato & Lynette I. Millett eds., 2010) (explaining that the primary purpose of a biometric system is to capture, store, and match biometric data).

purposes, including security, authentication of employee timekeeping, fraud prevention, and convenience.[9] The use of biometric data also brings challenges, including privacy and security concerns.[10]

In 2008, the Illinois legislature adopted the Biometric Information Privacy Act (BIPA) to regulate businesses' collection of biometric information.[11] As stated in the statute, its goal is to protect the biometric information of private individuals.[12] BIPA provides standards for businesses in collection, use, safeguarding, handling, storage, retention, and destruction of biometric identifiers and information.[13] The statute does not prevent companies from using biometric data, but it does limit the way in which businesses use the information.[14] Under BIPA,

9. *See* McCray, *supra* note 2, at 77 ("An increasing number of vendors, employers, and businesses—both large and small—are incorporating biometric data into their daily operations as mechanisms to streamline their systems, to prevent timekeeping fraud, and to bolster the strength and integrity of their operational security."); *What Is Biometrics?*, *supra* note 6 (demonstrating the use of biometrics in government and commercial settings by describing that biometric recognition is "used by financial institutions to prevent fraud, by citizens to secure their mobile phones, and by the Department of Homeland Security to enhance border security"); *see also* Dave Zielinksi, *Use of Biometric Data Grows, Though Not Without Legal Risks*, SHRM: TECH. (Aug. 23, 2018), https://www.shrm.org/resourcesandtools/hr-topics/technology/pages/biometric-technologies-grow-.aspx (identifying companies' use of biometric data as a way to authenticate employee identity for timekeeping).

10. Zimmerman, *supra* note 2, at 656 ("This constant tracking and collection of information poses a myriad of potential harms to consumers. Companies that collect and store aggregations of consumer data are at risk for security breaches where personal information is accessed by hackers."); *see also* Chiara A. Sottile, *As Biometric Scanning Use Grows, So Does Security Risk*, NBC NEWS: MACH (July 24, 2016, 6:29 PM), https://www.nbcnews.com/mach/mach/biometric-scanning-use-grows-so-do-security-risks-ncna593161.

11. *See Illinois Biometric Information Privacy Act FAQs*, JACKSON LEWIS (2017), https://www.jacksonlewis.com/sites/default/files/docs/IllinoisBiometricsFAQs2017.pdf [hereinafter *BIPA FAQs*] (discussing that Illinois was one of the first states to pass a law regulating businesses' use of biometric data); *see also What Is BIPA? Biometric Information Privacy Act*, PEIFFER WOLF CARR & KANE, https://prwlegal.com/practice-areas/biometric-information-privacy-act/ (last visited June 16, 2019) [hereinafter *What Is BIPA?*] (discussing the adoption of BIPA).

12. *See* 740 ILL. COMP. STAT. 14/5 (2018) (describing the sensitive nature of an individual's biometric data and stating that the statute's protection of such data will benefit public welfare, security, and safety).

13. *See BIPA FAQs*, *supra* note 11 (describing that the key features of BIPA are informed consent prior to collection, a limited right to disclosure, protection obligations and retention guidelines, prevention of profiting from biometric data, a private right of action for individuals harmed by BIPA violations, and statutory damages that can reach $1,000 for each negligent violation and $5,000 for each intentional or reckless violation); Justin O. Kay, *The Illinois Biometric Information Privacy Act*, ASS'N CORP. COUNS. 1–2 (2017), https://m.acc.com/chapters/chic/upload/Drinker-Biddle-2017-1-BIPA-Article-2.pdf (detailing the sections of BIPA); *What Is BIPA?*, *supra* note 11 (describing statute elements).

14. *See What is BIPA?*, *supra* note 11 (describing the elements of compliance for businesses); *see also BIPA FAQs*, *supra* note 11 (suggesting a comprehensive plan for businesses to comply with BIPA).

companies must give notice and collect consent from individuals, companies cannot sell biometric data, and companies must develop policy for reasonable care in retention and destruction of information.[15] BIPA also creates a private right of action, so aggrieved individuals may file suit against entities for violation of the statute.[16]

From 2008 until 2015, BIPA was a relatively unknown statute.[17] In 2015, its anonymity ended when a wave of lawsuits were filed under BIPA.[18] In 2017, the number of lawsuits filed under BIPA exploded as employees began suing their employers.[19] As the body of law on BIPA progressed, a new issue regarding an individual's standing emerged.[20]

15. *See* Erin Marine, *Biometric Privacy Laws: Illinois and the Fight Against Intrusive Tech*, FORDHAM J. CORP. & FIN. L. BLOG (Mar. 20, 2018), https://news.law.fordham.edu/jcfl/2018/03/20/biometric-privacy-laws-illinois-and-the-fight-against-intrusive-tech/ ("Under the Act, companies must give notice when they are collecting, using or storing biometric information, and must obtain written consent before collecting biometric data from any individual. . . . More specifically, companies must develop and implement a written biometric data policy that details guidelines for the retention and destruction of biometric data and adopt procedural safeguards to ensure sensitive data isn't leaked or stolen."); s*ee also* Erica Gunderson, *Biometric Data: Are We Safer in Illinois, or Just Having Less Fun?*, WTTW NEWS: SCI.-TECH. (Jan. 22, 2018, 5:07 PM), https://chicagotonight.wttw.com/2018/01/22/biometric-data-are-we-safer-illinois-or-just-having-less-fun (stating that BIPA "bars the sharing of the data with others except in very narrow circumstances, and bars (without exception) the sale or profiting from the data").

16. *See A New Threat from an Old Source: Class Action Liability Under Illinois' Biometric Information Privacy Act*, BAKER MCKENZIE (Oct. 16, 2017), https://www.bakermckenzie.com/en/insight/publications/2017/10/illinois-biometric-information-privacy-act [hereinafter *A New Threat from an Old Source*] (stating that individuals can file suit under BIPA for statutory violations related to the collection, retention, storage, and use of biometric identifiers and information); *see also* Gunderson, *supra* note 15 (explaining that "BIPA permits individuals to sue in court for violations of BIPA in certain circumstances").

17. *See* Insler, *supra* note 5, at 35 ("In December 2015, the U.S. District Court for the Northern District of Illinois noted that it was 'unaware of any judicial interpretation of the statute.'" (quoting Norberg v. Shutterfly, Inc., 152 F. Supp. 3d 1103, 1106 (N.D. Ill. 2015))).

18. *See* Mimi Moore et al., *Biometric Privacy Targeted in Increased Class Action Litigation in Illinois*, BRYAN CAVE LEIGHTON PAISNER (Nov. 17, 2017), https://www.bryancave.com/en/thought-leadership/biometric-privacy-targeted-in-increased-class-action-litigation.html ("The BIPA, however, was largely ignored until mid-2015 when the first wave of BIPA litigation was filed against social media and photo-storage/sharing services."); *see also* Carley Daye Andrews et al., *Litigation Under Illinois Biometric Information Privacy Act Highlights Biometric Data Risks*, K&L GATES (Nov. 7, 2017), http://www.klgates.com/litigation-under-illinois-biometric-information-privacy-act-highlights-biometric-data-risks-11-07-2017 ("Despite years of inactivity under Illinois BIPA, seven cases were filed in 2015; plaintiffs then filed seven more putative class actions in 2016.").

19. *See* Jay Hux, *Collecting Employee Biometric Data Could Prove Costly in Illinois*, SHRM: ST. & LOC. UPDATES (Sept. 19, 2017), https://www.shrm.org/resourcesandtools/legal-and-compliance/state-and-local-updates/pages/collecting-employee-biometric-data-could-prove-costly-in-illinois.aspx ("The increased use of biometric data has led to a series of class-action lawsuits in Illinois alleging employer violations of the BIPA."); *see also A New Threat from An Old Source*, *supra* note 16 (explaining that from July 2017 to October 2017, there were more than twenty-five BIPA cases filed in the state and federal courts in Illinois).

20. *See* Jeffrey Neuburger, *Litigants Alleging Procedural Violations of Illinois Biometric Privacy Statute (BIPA) Are Not "Aggrieved" Parties That May Seek Legal Remedies*, PROSKAUER

Three notable cases in Illinois were decided, the central holdings of which defined what it meant for an individual to have standing under BIPA.[21] These decisions defined the meaning of an "aggrieved party" as used in the BIPA statute.[22] In *McCollough v. Smarte Carte, Inc.*[23] and *Rosenbach v. Six Flags Entertainment Corp.*,[24] the courts found that an individual is not an aggrieved party if she alleges a technical violation without showing actual harm or injury.[25] However, the Illinois Appellate Court in *Sekura v. Krishna Schaumberg Tan, Inc.*[26] found otherwise, and held that a technical violation of BIPA could cause a party to be aggrieved.[27] As a result, uncertainty and a need for clarification existed on this issue.[28]

ROSE LLP: NEW MEDIA & TECH. L. BLOG (Jan. 2, 2018), https://newmedialaw.proskauer.com/2018/01/02/litigants-alleging-procedural-violations-of-illinois-biometric-privacy-statute-bipa-are-not-aggrieved-parties-that-may-seek-legal-remedies/. In 2017,

> it was not clear if mere procedural violations of BIPA's consent and data retention requirements, without any showing of actual harm or data misuse, were actionable under the statute (i.e., whether persons pleading procedural violations are 'aggrieved' under the statute, as BIPA expressly provides that 'any person aggrieved by a violation' of the BIPA may pursue money damages and injunctive relief against the offending party).

Id.

21. *See* Insler, *supra* note 5, at 49 (identifying McCollough v. Smarte Carte, Inc., No. 16 C 03777, 2016 WL 4077108 (N.D. Ill. Aug. 1, 2016), Rosenbach v. Six Flags Entm't Corp., 2017 IL App (2d) 170317, *rev'd*, 2019 IL 123186, and Sekura v. Krishna Schaumburg Tan, Inc., 2018 IL App (1st) 180175).

22. *See* 740 ILL. COMP. STAT. 14/20 (2018) ("Right of action. Any 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."); *see also, e.g.*, Insler, *supra* note 5, at 37 (providing background on decisions made in Illinois regarding "aggrieved party" language).

23. 2016 WL 4077108.

24. 2017 IL App (2d) 170317.

25. *See* Insler, *supra* note 5, at 49 ("Reviewing *McCollough*, Black's Law Dictionary, and other authorities, the second district held that if 'a person alleges only a technical violation of the Act without alleging any injury or adverse effect, then he or she is not aggrieved and may not recover . . . .'" (quoting *Rosenbach*, 2017 IL App (2d) 170317, ¶ 28)); *see also* Andrew Goldstein, *Collecting Fingerprints or Other Biometric Information Without Consent Could Be Costly*, FREEBORN (Oct. 13, 2017), https://www.incubateillinois.com/2017/10/collecting-fingerprints-biometric-information-without-consent-costly ("Smarte Carte argued that the plaintiffs lacked standing to bring the claims based on a mere procedural violation of the BIPA without the plaintiffs suffering any actual damages. The court agreed and dismissed the case asking, 'How can there be an injury from the lack of advance consent to retain the fingerprint data beyond the rental period if there is no allegation that the information was disclosed or at risk of disclosure?'" (quoting *McCollough*, 2016 WL 4077108, at *3)).

26. 2018 IL App (1st) 180175.

27. *See* Insler, *supra* note 5, at 37, 49 ("[T]he Circuit Court of Cook County found Sekura was 'aggrieved' within the meaning of the statute. The judge wrote that the term 'aggrieved' does not require a plaintiff to plead 'specific or actual damages' and is to be given a broad reading to protect 'anyone like the plaintiff [] whose personal information has allegedly been mishandled in violation of BIPA'" (quoting Sekura v. Krishna Schaumberg Tan, Inc., No. 2016 CH 4945, 2017 WL 1181420, at *3 (Ill. Cir. Ct. Feb. 9, 2017))).

28. *See* Micha Nandaraj Gallo, *Illinois Supreme Court to Decide Statutory Standing Requirements Under the Illinois Biometric Information Privacy Act*, COVINGTON (Nov. 21, 2018), https://www.insideprivacy.com/data-privacy/illinois-supreme-court-to-decide-statutory-standing-

On January 25, 2019, the Illinois Supreme Court provided clarity by resolving the inter-district split on what it means to be an "aggrieved party." In a unanimous decision in *Rosenbach v. Six Flags*,[29] the court held a person is "aggrieved" when there is a technical violation of BIPA; a showing of further harm is not necessary to bring a cause of action under the statute.[30]

To reach its decision, the Illinois Supreme Court interpreted the plain meaning of BIPA's language, analyzed the legislative intent of the statute, compared BIPA to other Illinois statutes, and consulted analogous Illinois cases.[31] The Illinois Supreme Court's decision ultimately reflects the purpose of BIPA: the protection of an individual's rights to private biometric information and the prevention of insecure technology use by companies.[32] Although some critics of the decision fear a boom in litigation and damage to businesses, the benefits of the court's interpretation outweigh any potential negatives. In addition, this decision correctly placed greater importance on data privacy and reflects a growing trend of concern over privacy.

Part I will discuss the evolution of biometric technology and its multiple uses by business.[33] This section will also explore the benefits of biometric data as well as concerns that have led to the enactment of legislation regarding biometric data.[34]

Part II will analyze the significant regulation on biometric privacy collection: BIPA.[35] Part II will also introduce different forms of litigation that occurred after the enactment of BIPA.[36] This section will also

---

requirements-under-the-illinois-biometric-information-privacy-act/ (observing that this decision presented the Illinois Supreme Court with an opportunity to resolve an inter-district split); *see also* Thomas Quinn Ford, *Illinois Supreme Court Holds No Showing of Actual Harm Needed to State Claim Under Biometric Information Privacy Act*, NAT'L L. REV. (Jan. 28, 2019), https://www.natlawreview.com/article/illinois-supreme-court-holds-no-showing-actual-harm-needed-to-state-claim-under ("The court's decision in *Rosenbach v. Six Flags* [] *Entertainment Corp.* settles a split among Illinois' appellate courts, which centered on what a plaintiff needs to plead to be considered 'aggrieved' under BIPA.").

29. *See generally* Rosenbach v. Six Flags Entm't Corp., 2019 IL 123186.

30. *Id.* ¶ 40; *see also* Monica R. Chmielewski et al., *Biometric Privacy: Illinois Supreme Court Decision Allows Claims to Proceed Without Showing of Actual Harm*, NAT'L L. REV. (Feb. 4, 2019), https://www.natlawreview.com/article/biometric-privacy-illinois-supreme-court-decision-allows-claims-to-proceed-without (providing an overview of the Illinois Supreme Court's decision).

31. *See infra* Parts III.A–D.

32. *See* 740 ILL. COMP. STAT. 14/5(c), (g) (2018) (describing the sensitive nature of an individual's biometric data and stating that the statute's protection of such data will benefit public welfare, security, and safety).

33. *See infra* Part I.A.

34. *See infra* Parts I.A–B.

35. *See infra* Part II.A.

36. *See infra* Parts II.B(1)–(2).

introduce the recent cases about BIPA's "aggrieved party" language and discuss the case law's interpretation of this statute.[37]

Part III will analyze the holding in *Rosenbach v. Six Flags Entertainment Corp.*[38] This section observes the interpretative principles the court used to reach its decision that a statutory violation creates an "aggrieved" party.[39] Part III also compares the Supreme Court's reasoning to the analysis used in lower court decisions.[40]

In Part IV, I suggest that BIPA should be construed as a statute that protects the individual's rights, and that the court's interpretation was in accordance with this view.[41] This section also explores the impact that this holding will have on future BIPA litigation and business and technology advancement.[42] In addition, this Part will observe the changing landscape of privacy laws nationwide.[43]

I. BIPA'S BACKGROUND

Biometrics can be used to recognize individuals based on their biological information. Businesses use biometric data for a multitude of reasons, including security, convenience, and monitoring of employees.[44] Although widely used, biometric systems also carry security risks and privacy concerns.[45] In response to these concerns, Illinois's legislature sought to protect the biometric data of its citizens by law.[46]

A. The Development of Biometric Data

Biometrics is the automated recognition of individuals based on their unique behavioral and biological characteristics.[47] The practice of identifying individuals by their biological information is not a new one;

37. *See infra* Part II.B(3).
38. *See infra* Parts III.A–D.
39. *See infra* Parts III.A–D.
40. *See infra* Parts III.A–D.
41. *See infra* Part IV.D.
42. *See infra* Parts IV.A–B.
43. *See infra* Part IV.C.
44. *See* McCray, *supra* note 2, at 77; *What Is Biometrics?*, *supra* note 6.
45. *See, e.g.*, Sottile, *supra* note 10 (discussing instances of biometric hacking where millions of individuals have lost personal information to identity theft).
46. Jacob Radecki & Christopher Dean, *Actual Injury Required to State a Claim Under Illinois Biometric Information Privacy Act*, MCDONALD HOPKINS: BUS. ADVOC. (Jan. 18, 2018), https://mcdonaldhopkins.com/Insights/Blog/Litigation-Trends/2018/01/18/Actual-injury-required-to-state-a-claim-under-the-Illinois-Biometric-Information-Privacy-Act ("BIPA was enacted in 2008 in response to concerns that consumers' fingerprints and other biometric data were being gathered, stored, and possibly sold by Illinois businesses.").
47. BIOMETRIC RECOGNITION: CHALLENGES AND OPPORTUNITIES, *supra* note 8, at 1 (defining the term "biometrics"). *See also, e.g.*, *DHS Biometrics*, *supra* note 6 (providing a general definition of "biometrics," and using one's fingerprints as an illustration).

fingerprints have been used for identification purposes for over a century.[48] The more modern form of biometric identification emerged in the 1960s, when the process of biometric identification became automated due to the increased availability of computers.[49] Today, fully automated systems can identify an individual by recognizing characteristics such as fingerprints, face, iris, voice, and behavioral characteristics.[50] A general biometric system performs two basic operations: (1) it creates a reference database when it captures and stores a new biometric sample and information on an individual, and (2) it matches information when it captures a sample and compares it to previously collected reference samples.[51]

The use of biometric data is widespread and growing, especially in the context of businesses collecting consumer and employee data.[52]

48. *See* BIOMETRIC RECOGNITION: CHALLENGES AND OPPORTUNITIES, *supra* note 8, at 16 (noting that British geneticist Francis Galton, who made important contributions to fingerprinting as a tool for identification of criminals, coined the term "biometry" in 1901); *see also What Is Biometrics?*, *supra* note 6 (stating that biometric recognition techniques have been used in forensic applications for over 100 years).

49. *See* BIOMETRIC RECOGNITION: CHALLENGES AND OPPORTUNITIES, *supra* note 8, at 16 (defining "automated" as the use of digital computers and explaining that automated fingerprint, handwriting, and facial recognition systems emerged in the 1960s as digital computers became more widespread and capable); *see also What Is Biometrics?*, *supra* note 6 (explaining that the first scientific paper on automated fingerprint matching was published by Mitchell Trauring in 1963).

50. *See What Is Biometrics?*, *supra* note 6 (describing anatomical and behavioral characteristics that biometric recognition utilizes); *see, e.g.*, *DHS Biometrics*, *supra* note 6 (illustrating biometric information using the example of an individual's fingerprints).

51. *See* BIOMETRIC RECOGNITION: CHALLENGES AND OPPORTUNITIES, *supra* note 8, at 2 (describing components of a system as "capture," where the sensor collects biometric data from the subject to be recognized; the "reference database," where previously enrolled subjects' biometric data are held; the "matcher," which compares presented data to reference data in order to make a recognition decision; and "action," where the system recognition decision is revealed and actions are undertaken based on that decision); *What Is Biometrics?*, *supra* note 6 (illustrating a diagram on the biometric capture process); Zimmerman, *supra* note 2, at 641 ("The biometric information in the database is compiled as measurements, which are used to create an algorithm or a 'template' of an individual's specific biometric characteristic . . . . Once an individual's characteristic is in a database, it is compared to new records. Biometric authentication can then be used to either verify an individual's identity, or to identify an unknown person. If the new records match the database record, then that individual's identity is confirmed." (footnotes omitted)).

52. *See* Sottile, *supra* note 10 ("By 2019, biometrics are expected to be a 25-billion-dollar industry with more than 500 million biometric scanners in use around the world . . . ."); *see also* Zimmerman, *supra* note 2, at 637 ("The number of phones with embedded fingerprint sensors is projected to grow from 499 million in 2015 to 1.6 billion in 2020. By 2019, fifty percent of smartphones are expected to integrate an embedded fingerprint sensor." (footnote omitted)). *See* April Glaser, *Biometrics Are Coming, Along with Serious Security Concerns*, WIRED (Mar. 9, 2016, 11:00 AM), https://www.wired.com/2016/03/biometrics-coming-along-serious-security-concerns ("Since Apple introduced its incredibly usable biometric identification with Apple's home button fingerprint sensor in 2013, the appetite for biometrics has expanded rapidly. Now MasterCard wants to use your heartbeat data to verify purchases. Google's new Abicus Project plans to monitor your speech patterns, as well as how you walk and type, to confirm that it's really you on the other end of the smartphone. Other apps are looking at the uniqueness of vascular patterns in the eyes or

Businesses use biometric data for a variety of purposes including security, monitoring of employees, and convenience.[53] For purposes of security and fraud prevention, biometric data can be helpful for businesses and customers alike.[54] Traditional means of identification (such as passwords, driver's licenses, and social security numbers) can be forgotten, lost, or forged.[55] Instead of less secure protection methods like passwords, biometric data can be used to unlock mobile devices and mobile banking applications, prove identification at ATMs, and approve payment at retail point of sale systems.[56] This identification is more difficult to replicate and cannot be lost, because it is based on an individual's unique biological markers.[57] Additionally, employers can utilize biometric data to better monitor their employees and accurately clock their hours.[58] Companies are also beginning to incorporate

even a person's specific gait to verify identities."); *see also* Selena Larson, *Beyond Passwords: Companies Use Fingerprints and Digital Behavior to ID Employees*, CNN: BUS. (Mar. 18, 2018, 3:53 PM), https://money.cnn.com/2018/03/18/technology/biometrics-workplace/index.html (estimating that 90 percent of businesses will use biometric authentication by 2020).

53. *See* McCray, *supra* note 2, at 77; *What Is Biometrics?*, *supra* note 6; *see also* Zielinksi, *supra* note 9 (identifying companies' use of biometric data as a way to authenticate employee identity for time-keeping).

54. *See* Zimmerman, *supra* note 2, at 639; *see also* McCray, *supra* note 2, at 77.

55. *See* Zimmerman, *supra* note 2, at 642 ("Traditional methods of identification include passwords, personal identification numbers (PIN), driver's licenses, passports, and, increasingly, social security numbers. While these methods have been used for years, they have unavoidable disadvantages." (footnote omitted)).

56. *See* Larson, *supra* note 52 (noting that "[c]ompanies such as Microsoft (MSFT) and Facebook (FB) are trying to get rid of passwords completely," Microsoft has new software which "uses face scans or fingerprints to log in to Windows devices," that "[m]ore than 50 million people use Windows Hello to log in to their PCs," and Apple introduced the iPhone X, which uses facial recognition unlocking technology); *see also Biometric ATM*, BIOENABLE, https://www.bioenabletech.com/biometrics-atm (last visited June 16, 2019) (describing biometric enabled ATMs); Justin Lee, *Juniper Research Projects Nearly 5 Billion Biometric Transactions by 2019*, BIOMETRICUPDATE.COM (Oct. 27, 2015), https://www.biometricupdate.com/201510/juniper-research-projects-nearly-5-billion-biometric-transactions-by-2019 (citing reports that the increased use of touchless payment services such as Apple Pay and Samsung Pay that use fingerprint readers will increase the number of biometric authenticated transactions to nearly 5 billion by 2019).

57. *See* Zimmerman, *supra* note 2, at 642 ("[B]iometric identification is difficult to duplicate, cannot be lost, and does not depend on an individual to remember it because it is based on his or her 'intrinsic characteristics.' Biometric characteristics are inherent and provide completely unique data sets that result in accurate data generation and verification. It is, in fact, these intrinsic characteristics that appeal so strongly to innovators." (footnotes omitted)); *see also* Tiffany Lee, *Biometrics and Disability Rights: Legal Compliance in Biometric Identification Programs*, 2016 U. ILL. J.L. TECH. & POL'Y 209, 211 ("Biometric data has some advantages over the traditional methods of determining identity. Unlike passwords or identification cards, 'biometric identifiers cannot be shared or misplaced, and they intrinsically represent the individual's bodily identity.'").

58. *See* Hux, *supra* note 19 (explaining that companies use biometric devices as a more secure way to authenticate employee identity for time-keeping, to grant access to sensitive data, or to facilitate onboarding and offboarding. Companies use biometric systems to ensure that workers using a time clock are who they say they are and to avoid "buddy punching." Biometric time clocks

biometrics to add convenience and speed to their business practices in areas like security lines, restaurant food service, and age and identity certification.[59]

The increased use of biometrics demonstrates that the technology has real benefits for businesses and consumers.[60] However, while biometric technology can deliver convenience, experts acknowledge that the technology presents serious privacy and security concerns.[61] The technology is not perfectly secure, and there is always a possibility that the information can be hacked.[62] Companies who collect and store data are at risk for security breaches, and large cyber security breaches have

---

that use fingerprint scanning or facial recognition can also help HR better comply with labor laws by ensuring employees clock in and out accurately.); *see also* J. Wilson & C.R. Wright, *Using Biometrics in the Workplace*, FISHER PHILLIPS (Jan. 6, 2014), https://www.fisherphillips.com/resources-newsletters-article-using-biometrics-in-the-workplace (describing that businesses utilize biometric data to prevent "buddy punching" to ensure that they are paying employees for actual time worked and to increase security).

59. *See CLEAR Partners with Seattle Seahawks, Sounders & Mariners to Launch Industry-Leading Biometric Payments & ID Check for Fast, Frictionless Concessions*, BUS. WIRE (Aug. 6, 2018, 3:38 PM), https://www.businesswire.com/news/home/20180806005577/en/CLEAR-Partners-Seattle-Seahawks-Sounders-Mariners-Launch (announcing Seattle major sports teams' use of biometric information for age and identification verification in alcohol and concession purchases); *You're the Perfect Person to Verify Your Identity*, CLEAR, https://www.clearme.com/how-it-works (last visited June 16, 2019) (describing the company Clear, which hosts biometric machines in airports and large venues to reduce security lines); *see also Malibu Poke Is Banking on Facial Recognition Payments*, PYMNTS.COM: RESTECH (Dec. 7, 2017), https://www.pymnts.com/restaurant-technology/2017/malibu-poke-facial-recognition-biometrics-payments/ (describing the use of biometrics in self-serve restaurant kiosks).

60. *See* Sottile, *supra* note 10 ("With biometrics, there's no need to memorize an unwieldy sequence of numbers and letters as with passwords—and consumers value that convenience. In a OnePoll/Gigya survey, 80 percent of consumers who expressed a preference said they think biometric authentication is more secure than traditional passwords, and 52 percent of consumers said they would choose anything but a traditional password when given the choice."); *see also* Gunderson, *supra* note 15 (stating that biometric data delivers convenience and security to consumers).

61. *See* Robee Krishan & Reza Mostafavi, *Biometric Technology: Security and Privacy Concerns*, 22 J. INTERNET L. 19, 19 (2018) ("The concerns come in the form of both security and privacy. For instance, in the event of a data breach or hack, biometric data cannot be reissued, unlike the way passwords can be quickly changed following being compromised. Thus, the applications that make use of the biometrics will become defunct, until a new authentication method can be secured. This represents a material security flaw, but moreover there are also material privacy concerns. For example, biometric data contain information about individuals such as proclivity to certain diseases that could be used to discriminate in the form [of] insurance denial."); *see, e.g.*, Sottile, *supra* note 10 (discussing instances of widespread security breaches where sensitive biometric information was stolen).

62. *See* Glaser, *supra* note 52 (describing hacking events such as the 2015 hack of the U.S. Office of Personnel Management where 5.6 million people's fingerprints were compromised and referencing the findings of researchers and security firms in the penetrability of biometric security); *see also* Olivia Solon, *The End of Passwords: Biometrics Are Coming but Do Risks Outweigh Benefits?*, GUARDIAN (Dec. 8, 2015, 8:00 AM), https://www.theguardian.com/technology/2015/dec/08/the-end-of-passwords-biometrics-risks-benefits (describing the "tantalising" nature of personal data as evidenced by the 2015 OPM attack).

become increasingly common.[63] A biometric breach is especially problematic because, unlike passwords or social security numbers, biometric information cannot be erased or changed when personal information is compromised.[64] Additionally, some privacy advocates argue that biometric data deserves a higher level of protection than other personal information as it is so intimately tied to an individual.[65]

B. Adoption of the 2008 Biometric Information Privacy Act

BIPA was passed in 2008 in response to growing concerns regarding the security of consumers' biometric information.[66] Some of the concerns about the collection of biometrics stemmed from the collapse of a

63. *See* Zimmerman, *supra* note 2, at 656–57 ("As technology continues to evolve, a trend of increased cyber security breaches has emerged. . . . [R]ecently, the Philippines' Commission on Elections was subject to hackers who accessed a database of 55 million voters in the Philippines. Described as the largest government-related data breach in history, the leaked information included '228,605 email addresses; 1.3 million passport numbers and expiry dates of overseas Filipino voters; and 15.8 million fingerprint records.'" (footnotes omitted)); *see, e.g.*, Glaser, *supra* note 52 (noting personal data seized by the 2015 OPM attack); *see also* Paul J. Lim, *Equifax's Massive Data Breach Has Cost the Company $4 Billion So Far*, MONEY (Sept. 12, 2017), http://money.com/money/4936732/equifaxs-massive-data-breach-has-cost-the-company-4-billion-so-far/ (detailing the blow that Equifax suffered in the market due to a lack of trust in the company. Equifax's direct costs tied to dealing with this crisis were estimated between $200 million and $300 million.); Kevin McCoy, *Target to Pay $18.5M for 2013 Data Breach That Affected 41 Million Consumers*, USA TODAY (May 23, 2017, 4:10 PM), https://www.usatoday.com/story/money/2017/05/23/target-pay-185m-2013-data-breach-affected-consumers/102063932/ (explaining that Target is on the hook to pay an $18.5 million multistate settlement for the 2013 cyber-attack that compromised customer payment card accounts).

64. *See* Sottile, *supra* note 10 (quoting former Interpol and FBI member Marc Goodman, "You can always get a new credit card. You can always create a new password. [It's] really hard to get new fingers. You only have ten of them and once that information leaks, it's out and there's nothing you can do"); *see also* Zimmerman, *supra* note 2, at 658 ("Stolen biometric information poses unique problems for consumers. A victim of identity theft can get a new credit card, change their passwords and pin numbers, or even change their Social Security number. A victim of identity theft whose fingerprint data is stolen cannot change their fingerprints or get new ones. Biometric information is permanently associated with a user and once stolen, it is out of the user's control forever." (footnotes omitted)).

65. *See* Natasha Singer, *When a Palm Reader Knows More Than Your Life Line*, N.Y. TIMES (Nov. 10, 2012), https://www.nytimes.com/2012/11/11/technology/biometric-data-gathering-sets-off-a-privacy-debate.html (quoting advocates who suggest that biometric information should be handled as if it was a genetic sample); *see also What Facial Recognition Technology Means for Privacy and Civil Liberties: Hearing Before the Subcomm. on Privacy, Tech., & the Law of the S. Comm. on the Judiciary*, 112th Cong. 1 (2012) (statement of Al Franken, U.S. Sen.) ("I believe that we have a fundamental right to control our private information, and biometric information is already among the most sensitive of our private information, mainly because it is both unique and permanent.").

66. 740 ILL. COMP. STAT. 14/5(d) (2018) ("An overwhelming majority of members of the public are weary of the use of biometrics when such information is tied to finances and other personal information."); *see* Radecki & Dean, *supra* note 46 ("BIPA was enacted in 2008 in response to concerns that consumers' fingerprints and other biometric data were being gathered, stored, and possibly sold by Illinois businesses.").

company called Pay By Touch.[67] This company permitted consumers to link their bank accounts to their fingerprints, but it went out of business in early 2008.[68] The company's bankruptcy caused legislators to ask questions about the biometric information Pay By Touch collected and stored, because in its bankruptcy proceedings, the company sold its database that contained fingerprint data of thousands of Illinois residents without informing users how the data would be used.[69]

BIPA was introduced to the Illinois Senate in February 2008, and Representative Kathleen Ryg, BIPA's House sponsor, referred to the Pay By Touch incident as demonstrative of the necessity of protecting individuals' biometric data.[70] The fact that the company's users were unaware that their data was being sold and were provided no guarantee of security or protection helped the Illinois legislature realize that the state was in "very serious need of protections for the citizens of Illinois when it comes to biometric information."[71] In the hearing, there were no questions or discussion, and the bill proceeded immediately to a vote and unanimously passed in the House.[72]

BIPA's stated purpose also reflects an intent to safeguard and monitor individuals' data.[73] The statute first recognizes the personal nature of

67. *See* Gunderson, *supra* note 15 (discussing that the fall of Pay By Touch concerned customers that had provided their data to the company, but did not know what would become of their information); *see also* Insler, *supra* note 5, at 35 (noting that before its collapse, Pay By Touch operated the largest fingerprint scan system in Illinois and that a number of grocery stores, gas stations, and school cafeterias participated in its pilot program).

68. *See* Kay, *supra* note 13, at 1 ("Investors poured $340 million into the venture, and millions of consumers signed up. By late 2007, however, Pay By Touch and one of its founders—John Rogers—were mired in controversy and litigation (including bankruptcy), and in March 2008, Pay By Touch ceased all operations."); *see, e.g.*, Insler, *supra* note 5 (recounting the demise of Pay By Touch, which ultimately prompted the Illinois Legislature to enact BIPA).

69. *See* Insler, *supra* note 5, at 35 ("Pay By Touch's bankruptcy left thousands of individuals wondering what would become of their fingerprints, a form of biometric data . . . ."); *see, e.g.*, Kay, *supra* note 13, at 1 n.1 (quoting Illinois House Representative Joseph M. Lyons mentioning the pending uncertainty of former Pay By Touch customers as a motivating factor for the passage of BIPA).

70. *See* H.R. Debate Transcript, 95th Gen. Assemb. No. 276, at 249 (Ill. 2008) (statement of Rep. Kathy Ryg) ("This Bill is especially important because one of the companies that has been piloted in Illinois, Pay By Touch, is the largest fingerprint scan system in Illinois and they have recently filed for bankruptcy and wholly stopped providing verification services in March of 2008. This pullout leaves thousands of customers from Albertson's, Cub Foods, Farm Fresh, Jewel Osco, Shell, and Sunflower Market wondering what will become of their biometric and financial data.").

71. *Id.* (Statement of Rep. Joseph M. Lyons); *see* Kay, *supra* note 13, at 1 ("Pay By Touch's rise and fall was the catalyst for first state law governing the collection, use, safeguarding, and storage of biometric information . . . .").

72. *Id.* at 250 (statement of Rep. Joseph M. Lyons) ("On this Bill, there are 113 Members voting 'yes', 0 voting 'no'. This Bill, having received the Constitutional Majority, is hereby declared passed.").

73. 740 ILL. COMP. STAT. 14/5 (2018); *see also* Marine, *supra* note 15 (stating that that biometric privacy laws principally address corporations storing large swaths of the highly personal

biometric data by stating, "Biometrics are unlike other unique identifiers that are used to access finances or other sensitive information. For example, social security numbers, when compromised, can be changed. Biometrics, however, are biologically unique to the individual; therefore, once compromised, the individual has no recourse . . . ."[74] The statute also expresses concern over the lack of security and oversight of such information, and concludes that "[t]he public welfare, security, and safety will be served by regulating the collection, use, safeguarding, handling, storage, retention, and destruction of biometric identifiers and information."[75]

II. THE BIPA LITIGATION ROLLERCOASTER

BIPA was enacted in 2008 and has five notable provisions.[76] Illinois is one of only three states that has a statute protecting biometric data but BIPA is the only statute that provides a private cause of action.[77] In 2015, Illinois experienced an uptick of litigation under BIPA, and parties began bringing large class action suits against internet companies and employers.[78] For several years, the lower courts attempted to define what an "aggrieved party" meant and who had standing under BIPA, which resulted in an inter-district split, requiring the Illinois Supreme Court's intervention.[79]

A. Illinois's Biometric Information Privacy Act

Broadly stated, BIPA has five key features: (1) informed consent prior to collection; (2) a limited right to disclosure and prohibition of profiting from biometric data; (3) safeguarding regulations; (4) retention and destruction guidelines; and (5) a private right of action for individuals harmed by a BIPA violation with statutory damages that can reach $1,000 for each negligent violation, and $5,000 for each intentional or reckless

biometric data of consumers).

74. 740 ILL. COMP. STAT. 14/5(c).

75. *Id.* 14/5(g).

76. *Id.* 14; *see, e.g.*, *BIPA FAQs*, *supra* note 11 (outlining the practical effects of BIPA with regard to application for Illinois businesses and organizations); Insler, *supra* note 5, at 36 (discussing the origins and key provisions of BIPA).

77. *See* Andrews et al., *supra* note 18 (noting that BIPA has received more attention from plaintiffs compared to Texas or Washington's statutes, because BIPA has a private right of action while the Texas and Washington statutes do not); *see also* Insler, *supra* note 5, at 36 (highlighting that Illinois is the only state with a private cause of action for a biometric statute).

78. *See, e.g.*, Andrews et al., *supra* note 18 (tracking the recent increase in both individual and class action suits claiming violations of BIPA).

79. *See, e.g.*, Insler, *supra* note 5, at 37 (discussing the inter-district disagreement as to what constitutes an "aggrieved" person under BIPA, which encouraged the Illinois Supreme Court to provide guidance).

violation.[80]

First, relating to informed consent, BIPA prohibits any private entity from collecting, capturing, purchasing, or otherwise obtaining a person's biometric identifiers or information without first informing the individual or individual's authorized representative in writing that it is collecting data.[81] BIPA specifically defines biometric identifiers as "a retina or iris scan, fingerprint, voiceprint, or scan of hand or face geometry."[82] The entity must provide the specific purpose and length of term for which a biometric identifier or information is being collected, stored, and used.[83] Then, the private entity must also obtain a written release from the person in order to collect.[84]

Second, regarding sale and dissemination, BIPA prohibits any private entity from (1) selling, leasing, trading, or otherwise profiting from a biometric identifier or information; and (2) otherwise disclosing or disseminating such information unless the person consents, the disclosure completes a financial transaction authorized by the person, or the disclosure is required by law or requested via warrant or subpoena.[85]

Third, to ensure effective data safeguarding, BIPA requires any private

80. 740 ILL. COMP. STAT. 14 (2018); *see, e.g.*, *BIPA FAQs*, *supra* note 11 (discussing the five key elements of BIPA, including the monetary penalties for each violation of the statute); *see* Insler *supra* note 5, at 36 (discussing the five key features of BIPA).

81. 740 ILL. COMP. STAT. 14/15(b); *see, e.g.*, Kay, *supra* note 13, at 2 (highlighting the informed consent requirement of BIPA, along with what pieces of information must be included in the written consent form).

82. 740 ILL. COMP. STAT. 14/10.

> This statute notes that biometric identifiers do not include writing samples, written signatures, photographs, human biological samples used for valid scientific testing or screening, demographic data, tattoo descriptions or physical descriptions such as height, weight, hair color, or eye color . . . donated organs, tissues, or parts as defined in the Illinois Anatomical Gift Act or blood or serum stored on behalf of recipients or potential recipients of living or cadaveric transplants and obtained or stored by a federally designated organ procurement agency . . . materials regulated under the Genetic Information Privacy Act . . . information captured from a patient in a health care setting or information collected, used, or stored for health care treatment, payment, or operations under the federal Health Insurance Portability and Accountability Act of 1996 . . . an X-ray, roentgen process, computed tomography, MRI, PET scan, mammography, or other image or film of the human anatomy used to diagnose, prognose, or treat an illness or other medical condition or to further validate scientific testing or screening.

Id.

83. 740 ILL. COMP. STAT. 14/15(b)(2); *see, e.g.*, Kay, *supra* note 13, at 2 (detailing the consent form requirements that businesses and organizations must provide in order to comply with BIPA).

84. 740 ILL. COMP. STAT. 14/15(b)(3); *see, e.g.*, Kay, *supra* note 13, at 2 (noting BIPA's writing requirement that businesses and organizations must abide by in order to collect an individual's biometric information).

85. 740 ILL. COMP. STAT. 14/15(c)–(d); *see, e.g.*, Kay, *supra* note 13, at 2 (analyzing the strict prohibition against disseminating an individual's biometric information without their informed consent).

entity in possession of biometric identifiers or information to "store, transmit, and protect from disclosure all biometric identifiers and biometric information using the reasonable standard of care within the private entity's industry," and it must store the information in "the same as or more protective than the manner in which the private entity stores, transmits, and protects other confidential and sensitive information."[86]

Fourth, in retention and destruction, the private entity in possession of biometric identifiers or information must develop and adhere to

> 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.[87]

Lastly, BIPA creates a private right of action for "[a]ny person aggrieved by a violation of this Act" and entitles the prevailing party to recover $1,000 or actual damages (whichever is greater) for each negligent violation; $5,000 or actual damages (whichever is greater) for each intentional or reckless violation; reasonable attorneys' fees, litigation expenses, and costs (including expert witness fees); and "other relief, including an injunction" for each violation.[88]

Illinois was the first state to enact such a biometric protection statute and is unique compared to the other states that subsequently adopted biometric laws.[89] It is one of three states that have adopted an official policy on biometric privacy protection, with Texas and Washington being the other two states with biometric regulations statutes.[90] However, BIPA, unlike Washington's and Texas's statutes, allows for a private right of action.[91] In both Washington and Texas, there is no private right

86. Kay, *supra* note 13, at 2 (quoting 740 ILL. COMP. STAT. 14/15(e)).

87. *Id.* (quoting 740 ILL. COMP. STAT. 14/15(a)).

88. 740 ILL. COMP. STAT. 14/20.

89. *See* Becky Yerak, *Mariano's, Kimpton Hotels Sued over Alleged Collection of Biometric Data: 'It's Something Very Personal'*, CHI. TRIB. (July 21, 2017, 1:35 PM), http://www.chicagotribune.com/business/ct-employers-biometrics-lawsuits-0723-biz-20170720-story.html (describing Illinois as the first state to place restrictions on businesses' collection, storage, and use of biometric data and discussing that BIPA is considered the nation's toughest biometrics privacy law); *see, e.g.*, Marine, *supra* note 15 ("While two other states, Texas and Washington, have also implemented biometric privacy acts, BIPA remains the touchstone for biometric data regulation largely because of the significant penalties it imposes for noncompliance.").

90. *See* Paul Shukovsky, *Washington Biometric Privacy Law Lacks Teeth of Illinois Cousin*, BLOOMBERG BNA (July 18, 2017), https://perma.cc/ECA8-39HJ (explaining that Washington's 2007 biometric privacy law has significant compliance obligations but lacks a right for consumers to sue and that the 2009 Texas law doesn't include a provision to allow consumers to sue).

91. *See* Andrews et al., *supra* note 18 (noting that BIPA has received more attention from

of action, and enforcement of their respective biometric statutes is left to the state attorney general.[92] In addition, although biometric protection has been discussed at the federal level, no federal statute on biometric protection has been passed.[93]

Since BIPA's enactment, some have condemned the statute as deterrent to technological innovation, while others have criticized it for encouraging a wave of class actions.[94] In February 2018, Illinois Senator Bill Cunningham introduced a bill to amend BIPA.[95] The proposed bill responded to concerns about businesses' limited use of biometric data by allowing companies to collect employees' biometric information so long as the information is used exclusively for employment, human resources, identification, safety, security, or fraud prevention purposes.[96] This bill stalled in the Illinois Senate, and was instead delayed and re-referred in

---

plaintiffs than Texas or Washington's statutes because it has a private right of action while Texas and Washington statutes do not); *see also* Insler, *supra* note 5, at 36 (highlighting that Illinois is the only state with a private cause of action for a biometric statute).

92. *See, e.g.*, Andrews et al., *supra* note 18 (discussing the similarities and differences between Washington, Texas, and Illinois's respective statutes); Shukovsky, *supra* note 90 (highlighting the different characterizations of a private right of action allowance).

93. *See What Facial Recognition Technology Means for Privacy and Civil Liberties: Hearing Before the Subcomm. on Privacy, Tech., & the Law of the S. Comm. on the Judiciary*, 112th Cong. 3 (2012) (statement of Al Franken, U.S. Sen.) ("I called this hearing to raise awareness about the fact that facial recognition already exists right here, today, and we need to think about what that means for our society. I also called this hearing to call attention to the fact that our Federal privacy laws are almost totally unprepared to deal with this technology."); Zimmerman, *supra* note 2, at 243 ("Though the United States is a world leader in data-driven business, current federal statutes do not comprehensively regulate the collection of personal data via the Internet. Nor do they protect consumers from the collection of biometric data. There is no generally applicable federal law regulating the private industry's collection, storage, use, purchasing and selling of biometric information. Instead, federal privacy law in the United States is a patchwork of statutes that do not sufficiently protect individuals' biometric information privacy or give businesses a uniform law to follow." (footnote omitted)).

94. *See* Jeffrey Neuburger, *Illinois Considering Amendments to Biometric Privacy Law (BIPA) That Would Create Major Exemptions to Its Scope*, PROSKAUER: NEW MEDIA & TECH. L. BLOG (Apr. 17, 2018), https://newmedialaw.proskauer.com/2018/04/17/illinois-considering-amendments-to-biometric-privacy-law-bipa-that-would-create-major-exemptions-to-its-scope/ ("Privacy advocates have hailed BIPA's strong biometric privacy protections, while some in the tech and business community have decried that BIPA is deterring innovations in mobile services and spurring a wave of copycat litigation against companies that collect biometric data to authenticate customers or employees."); *see also* Ally Marotti, *Proposed Changes to Illinois' Biometric Law Concern Privacy Advocates*, CHI. TRIB. (Apr. 10, 2018, 4:55 PM), https://www.chicagotribune.com/business/ct-biz-illinois-biometrics-bills-20180409-story.html (quoting a critic of BIPA that stated "[e]mployers are being sued for minor technicalities of the law" and "[l]aws like the one currently in place also can add hoops for companies to jump through and inhibit investment in the state . . . when companies 'are looking to expand here, these sorts of laws are on their corporate white papers.'").

95. *See* S.B. 3053, 100th Gen. Assemb. (Ill. 2018); *see, e.g.*, Marotti, *supra* note 94 (reviewing some of the drawbacks of BIPA in its current form).

96. *See* Ill. S.B. 3053; *see, e.g.*, Marotti, *supra* note 94 (analyzing the claim that businesses are being sued for very minor violations).

April 2018.[97]

B. Recent Uptick in Litigation under BIPA

1. Large Class Action Lawsuits Against Internet Companies

From 2008 to 2015, BIPA was largely unknown to the legal community and rarely litigated.[98] This relative anonymity changed in 2015, however, when a series of cases against large social media and internet companies were brought under the statute.[99] These cases are significant because they demonstrated that BIPA could hold companies domiciled outside of the state accountable for information collected in Illinois. Additionally, the media coverage and notoriety these cases received drew more attention to BIPA.[100] *Norberg v. Shutterfly*[101] and *Rivera v. Google*[102] are two notable suits in this category.[103] Both cases involved class BIPA claims and were filed against large social media companies concerning facial recognition software.[104] In *Norberg*, the plaintiff filed suit on behalf of a class of people whose photographs and identifying information Shutterfly uploaded and stored without obtaining consent.[105] The U.S. district judge found that Norberg had successfully

97. *See* Ill. S.B. 3053.

98. *See* Insler, *supra* note 5, at 35 ("In December 2015, the U.S. District Court for the Northern District of Illinois noted that it was 'unaware of any judicial interpretation of the statute.'" (citing Norberg v. Shutterfly, Inc., 152 F. Supp. 3d 1103, 1106 (N.D. Ill. 2015))); *see also* Moore et al., *supra* note 18 (stating that BIPA was largely ignored until mid-2015 when the first wave of BIPA litigation was filed against social media and photo-storage/sharing services).

99. *See* Andrews et al., *supra* note 18 ("Despite years of inactivity under Illinois BIPA, seven cases were filed in 2015; plaintiffs then filed seven more putative class actions in 2016."); *see also* Moore et al., *supra* note 18.

100. *See Facing Privacy Suits About Facial Recognition: BIPA Cases Move Forward as More States Consider Passing Biometric Data Laws*, HUNTON ANDREWS KURTH: PRIVACY & INFO. SECURITY L. BLOG (Oct. 4, 2017), https://www.huntonprivacyblog.com/2017/10/04/facing-privacy-suits-about-facial-recognition-bipa-cases-move-forward-as-more-states-consider-passing-biometric-data-laws/ [hereinafter *Facing Privacy Suits*] (explaining that although in-store use of biometric-capture technology would currently pose a threat of consumer litigation only within Illinois, the *Norberg* and *Rivera* cases indicate that retailers can be sued for capturing or storing the biometric information of individuals accessing retailers' websites from within the state of Illinois); *see, e.g.*, Insler, *supra* note 5, at 37 (pointing out that large technology companies are not the only entities targeted by biometric security lawsuits).

101. Norberg v. Shutterfly, Inc., 152 F. Supp. 3d 1103 (N.D. Ill. 2015).

102. Rivera v. Google Inc., 238 F. Supp. 3d 1088 (N.D. Ill. 2017).

103. *See, e.g.*, Insler, *supra* note 5, at 37 (discussing initial judicial decisions interpreting BIPA including *Norberg* and *Rivera*); Kay, *supra* note 13, at 2.

104. *See, e.g.*, Insler, *supra* note 5, at 35 (noting that the court was "unaware of any judicial interpretation of the statute" (quoting *Norberg*, 152 F. Supp. 3d at 1106)); Kay, *supra* note 13, at 2.

105. *See* Kim Janssen, *Shutterfly Settles Facial Recognition Lawsuit With Man Who Claimed Privacy Violation*, CHI. TRIB. (Apr. 12, 2016, 2:57 PM), http://www.chicagotribune.com/business/ct-facial-recognition-lawsuit-0413-biz-20160412-story.html (describing allegations that

stated a claim under BIPA, and Shutterfly eventually settled.[106] Similarly, in *Rivera*, Google stored and scanned facial identifying information without the plaintiff class's consent.[107] The court rejected Google's argument that the application of BIPA would give the statute extraterritorial effect and violate the Dormant Commerce Clause, and found that any asserted violations must take place in Illinois to be actionable.[108]

2. Labor and Employment Lawsuits under BIPA

Shortly following these cases, a new wave of BIPA class action lawsuits were filed.[109] Notable defendants in these cases included Speedway, Inc., Roundy's, which operates the Mariano's grocery store chain, InterContinental Hotels Group, and Zayo Group.[110] Almost all the

---

Shutterfly "measured the contours of [Norberg's] face and the distance between his eyes, nose and ears to create a template it used to suggest other photos of Norberg be tagged with his name," and that it "attempted to determine Norberg's race, age and location without trying to get his consent, the suit alleged").

106. *See* Kim Janssen, *Facial Recognition Lawsuit Against Shutterfly Can Go Ahead, Judge Rules*, CHI. TRIB. (Jan. 13, 2016, 8:56 AM), http://www.chicagotribune.com/business/ct-shutterfly-lawsuit-0113-biz-20160112-story.html (explaining that "on December 29, 2015, U.S. District Judge Charges Norgle" ruled against Shutterfly's attempts to carry out the case and found that Norberg had "plausibly stated a claim" under BIPA); *see, e.g.*, Janssen *supra* note 105 (discussing the underlying facts and ultimate settlement of the *Norberg* case).

107. *Rivera*, 238 F. Supp. 3d at 1091 ("Based on these allegations, Rivera and Weiss, individually and on behalf of a proposed class, bring suit against Google for a violation of the Illinois Biometric Information Privacy Act. They argue that the face geometry templates created by Google are 'biometric identifiers' within the definition of the Privacy Act, and accordingly cannot be collected without consent.").

108. *See, e.g.*, *Facing Privacy Suits*, *supra* note 100 (citing *Rivera*, 238 F. Supp. 3d. at 1088); Jeffrey Neuburger, *Court Refuses to Dismiss Biometric Privacy Action over Facial Recognition Technology Used by Google Photos*, PROSKAUER: NEW MEDIA & TECH. L. BLOG (Mar. 2, 2017), https://newmedialaw.proskauer.com/2017/03/02/court-refuses-to-dismiss-biometric-privacy-action-over-facial-recognition-technology-used-by-google-photos/ (citing *Rivera*, 238 F. Supp. 3d. at 1088) (discussing cases interpreting the BIPA, including *Rivera*).

109. *See* Amy Korte, *Illinois Employers Flooded With Class-Action Lawsuits Stemming from Biometric Privacy Law*, ILL. POL'Y (Oct. 17, 2017), https://www.illinoispolicy.org/illinois-employers-flooded-with-class-action-lawsuits-stemming-from-biometric-privacy-law/ (explaining that between July and October 2017, employees filed twenty-six class action lawsuits against employers); *see also* Cynthia J. Larose, *The Law of Unintended Consequences: BIPA and the Effects of the Illinois Class Action Epidemic on Employers*, NAT'L L. REV. (Nov. 5, 2017), https://www.natlawreview.com/article/law-unintended-consequences-bipa-and-effects-illinois-class-action-epidemic ("Between July and October, nearly 26 class-action lawsuits were filed in Illinois state court by current and former employees alleging their employers had violated the BIPA. Companies range from supermarket chains, a gas station and convenience store chain, a chain of senior living facilities, several restaurant groups, and a chain of daycare facilities.").

110. *See, e.g.*, Korte, *supra* note 109 (listing Greencore USA-CPG Partners LLC, Superior Air-Ground Ambulance Service Inc., Millard Group LLC, Alliance Ground International LLC, Pineapple Hospitality Company and Pineapple Restaurant Group LLC, and ABRA Auto Body & Glass as additional employers that have been sued for alleged BIPA violations); Yerak, *supra* note 89 (discussing employers that "have been hauled into Cook County Circuit Court" in connection

suits filed involved employer time-keeping methods that used fingerprint or palm-print data to clock employees' work hours.[111] Plaintiffs alleged an array of BIPA violations, including lack of notice and written consent, and failure to inform about company policies for use, storage, and destruction of biometric data.[112] Most of these cases manifested as class action lawsuits, and plaintiff groups sought recovery of high dollar amounts.[113] These cases demonstrated potential for large class action recovery under BIPA, and the significant liability employers face if they fail to comply with the statute.[114]

3. Cases Defining "Aggrieved Party"

Beginning in 2016, BIPA litigation entered a new and impactful phase as defendants began to challenge the plaintiffs' standing, arguing they were not "aggrieved" within the meaning of the statute because they did not or could not allege an actual injury as a result of the defendant's violation of BIPA.[115] The statute specifies that "[a]ny person aggrieved

---

with alleged violations of BIPA).

111. *See* Korte, *supra* note 109 (explaining that "these lawsuits are largely based on the use of fingerprint-operated time clocks. The employee-plaintiffs have alleged their employers used those time clocks to collect, use and store biologically derived, or biometric, information in a manner that violates the consent, notice and disclosure requirements of the BIPA"); *see also* Larose, *supra* note 109 ("Facts vary from case to case, but nearly all of the recent employee BIPA cases implicate fingerprint or palm-print time-keeping technologies that collect biometric data to clock employees' work hours.").

112. *See* Korte, *supra* note 109 ("The plaintiffs allege their employers failed to inform employees about the companies' policies for use, storage and ultimate destruction of the fingerprint data or obtain the employees' written consent before collecting, using or storing the biometric information."); *see also* Yerak, *supra* note 89 (describing the reaction of Kipton hotel worker Eric Zepeda who joined in class action lawsuit: "'It's something very personal . . . . They were just calling us to put our finger' on a device. 'It seemed normal afterwards, but I was still uncomfortable and skeptical about it.' He said he doesn't know what Kimpton has done with his biometric data and worries about what would happen to his and his former co-workers' data if the company were to be bought or file for bankruptcy.").

113. *See* Hux, *supra* note 19 (stating that damages can be high because BIPA provides employees with the right to collect the greater of $1,000 or actual damages for each negligent violation, and the greater of $5,000 or actual damages for intentional or reckless violations); *see also* Yerak, *supra* note 89 (explaining that damages sought from Roundy's could exceed $7.5 million if 75 percent of its employees were to join the class action. If all workers became part of the class, potential damages could be $10 million).

114. *See* Hux, *supra* note 19 (advising employers by stating, "For now, employers that obtain or plan to obtain biometric data need to be aware of the BIPA's requirements and take steps to comply. These steps include providing employees with notice about biometric data collection and developing written policies related to the collection, retention and destruction of biometric data.").

115. *See Private Rights of Action Under Illinois Biometric Privacy Statute Sharply Limited*, ROPES & GRAY: NEWSROOM (Jan. 8, 2018), https://www.ropesgray.com/en/newsroom/alerts/2018/01/Private-Rights-of-Action-under-Illinois-Biometric-Privacy-Statute-Sharply-Limited [hereinafter *Private Rights of Action*] (defining the impact of *Rosenbach v. Six Flags Entertainment Corp.* as "a powerful tool for defendants to obtain dismissal of BIPA claims. Companies may often have arguments that their mere collection or other handling of biometric data caused no injury to

by a violation of this Act shall have a right of action."[116] However, in three cases, courts struggled to come to a consensus on what it means to be an "aggrieved party" within the meaning of the statute.[117] *McCollough v. Smarte Carte, Inc.*,[118] *Sekura v. Krishna Schaumberg Tan, Inc.*,[119] and *Rosenbach v. Six Flags Entertainment*[120] were the three cases that interpreted the meaning of "aggrieved party" prior to the Illinois Supreme Court in 2019.[121]

In 2016, *McCollough* was decided in the United States District Court for the Northern District of Illinois.[122] McCollough alleged that the defendant, Smarte Carte, a company that operates fingerprint activated lockers, retained her biometric information without notification and without her written consent.[123] Smarte Carte required that its customers scan their fingerprints in order to rent and unlock lockers.[124] It stored the customers' fingerprint data in order to recognize the customer for the unlocking process.[125] McCollough alleged that Smarte Carte failed to

---

plaintiff at all, requiring dismissal. Further, the ruling will likely make it harder for plaintiffs to obtain class certification under BIPA."); *see, e.g.*, Insler, *supra* note 5, at 37 (discussing the meaning of "aggrieved" within the statute).

116. *See* 740 ILL. COMP. STAT. 14/20 (2018) (describing the right of action of aggrieved persons).

117. *See* Goldstein, *supra* note 25 ("Courts have reached opposite results as to whether a plaintiff must show damages in order to have standing to bring a claim under Illinois' BIPA."); *Private Rights of Action*, *supra* note 115 ("[F]ederal district courts have reached conflicting conclusions as to whether a plaintiff must plead and prove actual adverse consequences from the alleged statutory violation in order to pursue his or her claims.").

118. McCollough v. Smarte Carte, Inc., No. 16 C 03777, 2016 WL 4077108 (N.D. Ill. Aug. 1, 2016).

119. Sekura v. Krishna Schaumburg Tan, Inc., 2018 IL App (1st) 180175.

120. Rosenbach v. Six Flags Entm't Corp., 2017 IL App (2d) 170317, *rev'd*, 2019 IL 123186.

121. *See, e.g.*, Goldstein, *supra* note 25 (discussing "aggrieved party"); Insler, *supra* note 5, at 37 (discussing the term "aggrieved party" within the meaning of the statute).

122. *McCollough*, 2016 WL 4077108. *See aso* Josh Kantrow, *Retaining Fingerprint Information Does Not Necessarily Violate the Illinois Biometric Act*, LEWIS BRISBOIS: ARTICLES (Aug. 30, 2016), https://lewisbrisbois.com/newsroom/articles/retaining-fingerprint-information-does-not-necessarily-violate-the-illinois (indicating that the case was decided in 2016).

123. *See McCollough*, 2016 WL 4077108, at *1 (explaining how the fingerprint is retained without any form of consent); *see also* Kantrow, *supra* note 122 (explaining that Smart Carte operates storage lockers that use the renter's fingerprints as a key. Plaintiff McCollough claimed to have used a Smart Carte locker at a train station five times in 2015).

124. *See McCollough*, 2016 WL 4077108, at *1 ("In order to rent a Smarte Carte locker . . . the customer is . . . instructed to place their finger on a fingerprint scanner, which is then displayed on the screen; finally, the screen displays the locker number and unlocks the locker. The lockers automatically lock when they are closed after the customer places their belongings inside."); *see, e.g.*, Kantrow, *supra* note 122 (discussing how renter's fingerprints are used as a key to operate storage lockers in Chicago).

125. *See McCollough*, 2016 WL 4077108, at *1 ("To retrieve their belongings, the customer selects from the touchscreen the option to open their rented locker. The customer places their finger on the scanner, which scans their fingerprint and displays it on the touchscreen. The matched fingerprint causes the customer's rented locker to unlock. The screen instructs the customer to

obtain written consent to record, collect, obtain or store its customers' fingerprints, did not inform its customers of the length of time it was retaining their information, and did not disclose how it protects or destroys biometric data.[126] McCollough did not allege that Smarte Carte illegally managed her information.[127]

Smarte Carte filed a motion to dismiss for lack of jurisdiction and failure to state a claim, and the district court granted its motion.[128] First, the court found that McCollough did not have subject matter jurisdiction because she failed to allege an injury that would give her standing under Article III of the Constitution.[129] The court held that McCollough did not have the requisite concrete harm to have standing under Article III because she did not allege more than a procedural violation.[130]

Next, the court briefly addressed McCollough's standing in Illinois

---

retrieve their belongings from the locker and the locker locks automatically when closed."); *see, e.g.*, Kantrow, *supra* note 122 (describing how the storage locker operation retained fingerprints).

126. *See McCollough*, 2016 WL 4077108, at *1 ("According to the Complaint, at no point does Smarte Carte inform customers and obtain their written consent to record, collect, obtain, or store their fingerprint. Smarte Carte also does not inform its customers of the length of time it retains the information. The Complaint alleges that Smarte Carte does not publicly disclose its retention schedule or guidelines for permanently destroying biometric identifiers and information. It also alleges that Smarte Carte has not disclosed the purpose and length of time for which the biometric identifiers and information is being collected, stored, and used." (citing Plaintiff's complaint)); *see also* Kantrow, *supra* note 122 (describing plaintiff's complaint, "She asserted that after retrieving her items from the locker, Smart Carte retained her biometric information (fingerprints) without notification and without her written consent."); Amy Korte, *Federal District Court in Illinois Dismisses Biometric Information Privacy Case Against Smarte Carte*, ILL. POL'Y (Aug. 19, 2016), https://www.illinoispolicy.org/federal-district-court-in-illinois-dismisses-biometric-information-privacy-case-against-smarte-carte/ ("The plaintiff in the Smarte Carte case alleged Smarte Carte failed to obtain her consent to collect, store and use her fingerprint, and did not provide information regarding the storage of her fingerprint.").

127. *See* Kantrow, *supra* note 122 (discussing that plaintiffs will need to allege more than a technical violation of BIPA, unlike the plaintiff in this case); *see, e.g.*, Goldstein, *supra* note 25 (describing that the court dismissed the case due to the lack of allegation that the information was disclosed or at risk of disclosure).

128. *See McCollough*, 2016 WL 4077108, at *1 ("Plaintiff, Adina McCollough, filed a three-count Complaint for damages, injunctive relief, and unjust enrichment stemming from violations of the Illinois Biometric Information Privacy Act ("BIPA"), 740 ILCS 14/1 *et seq.* Smarte Carte, Inc., now moves to dismiss for lack of jurisdiction and failure to state a claim. . . . [T]his Court grants the motion."); *see, e.g.*, Goldstein, *supra* note 25; Kantrow, *supra* note 122.

129. *McCollough*, 2016 WL 4077108, at *4 (holding that McCollough did not have standing under Article III of the Constitution because she did not show an injury in fact that was concrete and particularized).

130. *Id.* The court noted that "[e]ven without prior written consent to retain, if Smarte Carte did indeed retain the fingerprint data beyond the rental period, this Court finds it difficult to imagine, without more, how this retention could work a concrete harm." *Id.* (citing Gubala v. Time Warner Cable, Inc., No. 15-cv-1078, 2016 WL 3390415, at *4 (E.D. Wis. June 17, 2016) (finding that the plaintiff had not alleged a concrete injury as a result of the defendant retaining his personally identifiable information even though it was a technical violation of the Cable Communications Policy Act)).

under BIPA.[131] The court found that she was not an "aggrieved party" because she did not allege a real injury or adverse effect from the use of her fingerprints, even though Smarte Carte had committed a "technical violation" of BIPA by failing to obtain advance notice and failing to inform the McCollough of the company's retention policy.[132] The court found that a technical violation did not constitute an injury or adverse effect and that an individual is not "aggrieved" under BIPA if they do not experience more than a technical violation of BIPA.[133]

In 2017, the Cook County Circuit Court in *Sekura v. Krishna Schaumberg Tan, Inc.* reached a different conclusion and found that a mere technical violation of BIPA was sufficient to convey standing.[134] The defendant, Krishna Schaumberg Tan, Inc. (Krishna), filed a motion to reconsider, and in January 2018 the court reversed its 2017 decision, finding that a plaintiff needed to show more than a technical violation to have standing.[135] Sekura filed an appeal, and in September 2018, the Appellate Court of the First District of Illinois reversed the January 2018 decision and found that the original 2017 judgment was correct—that a plaintiff need only show a technical violation of BIPA to have standing.[136]

Sekura had a tanning membership with Krishna, a tanning salon that

131. *McCollough*, 2016 WL 4077108, at *4; *see, e.g.*, Insler, *supra* note 5, at 37 (discussing the McCollough's lack of actual injury as required by Article III); *see also* Neuburger, *supra* note 20 and accompanying text.

132. *McCollough*, 2016 WL 4077108, at *4 ("McCollough . . . has not alleged any facts to show that her rights have been adversely affected by the violation. She is essentially claiming that the very fact of a technical violation is the adverse effect. Accordingly, this Court finds that McCollough also lacks statutory standing.").

133. *Id.*; *see also id.* at *3 ("How can there be an injury from the lack of advance consent to retain the fingerprint data beyond the rental period if there is no allegation that the information was disclosed or at risk of disclosure?").

134. *See* Sekura v. Krishna Schaumburg Tan, Inc., 2018 IL App (1st) 180175, ¶ 3 ("Initially, the trial court denied defendant's motion to dismiss, finding that under the plain language of the statute plaintiff was a person aggrieved by a violation of the Act."); *see also* Insler, *supra* note 5, at 37 (explaining that the court dismissed defendant's motion).

135. *See Sekura*, 2018 IL App (1st) 180175, ¶¶ 3–5, 18–19 (explaining the procedural history of this case); *see, e.g.*, Jeffrey Neuburger, *Illinois Biometric Privacy Suit Survives Dismissal Based on Harm from Alleged Disclosure of Data to Outside Vendor*, PROSKAUER: NEW MEDIA & TECH. L. BLOG (June 21, 2018), https://newmedialaw.proskauer.com/2018/06/21/illinois-biometric-privacy-suit-survives-dismissal-based-on-harm-from-alleged-disclosure-of-data-to-outside-vendor/ (mentioning the brief order dismissing the claims).

136. *Sekura*, 2018 IL App (1st) 180175, ¶¶ 4–5 (holding that the trial court was initially correct); *see also IL Supreme Court Decides to Take Up Six Flags Fingerprint Privacy Case; Spurs Fresh Rise in BIPA Lawsuits*, COOK COUNTY REC. (June 29, 2018), https://cookcountyrecord.com/stories/511470207-il-supreme-court-decides-to-take-up-six-flags-fingerprint-privacy-case-spurs-fresh-rise-in-bipa-lawsuits [hereinafter *Fresh Rise in BIPA Lawsuits*] (explaining that the Second District Appellate Court sided with the plaintiffs, that a simple technical violation of Illinois BIPA law is sufficient).

used customers' fingerprint scans for membership ID purposes.[137] When Sekura bought a tanning package with Krishna, it required her to scan her fingerprint.[138] Krishna stored these scans and disclosed them to a third-party vendor.[139] Sekura alleged that Krishna violated BIPA by not informing her of the purpose or length or time it would use and store her information, for failing to inform her of its retention and destruction policy, and by failing to obtain her written consent to collect, store, and disclose her information to a third party.[140] Additionally, Krishna's franchisor had serious financial troubles, and Sekura alleged that she suffered from emotional harm and anguish because she did not know what would happen to her data if Krishna or its franchisor went bankrupt.[141]

In 2016, Krishna moved to dismiss for a failure to state a cause of action.[142] The trial court denied its motion and found that Sekura did not have to show damages other than the mishandling of her information in order to be aggrieved.[143] A "technical violation" was found to be sufficient to state a claim under BIPA.[144] The trial court interpreted the

137. *Sekura*, 2018 IL App (1st) 180175, ¶¶ 7–8; *see, e.g.*, Insler, *supra* note 5, at 37 (describing Sekura's allegation that the fingerprints for identification purses were required and that she had not been adequately informed).

138. *Sekura*, 2018 IL App (1st) 180175, ¶ 7 ("When a customer first purchases services at defendant's tanning salon, he or she is enrolled in L.A. Tan's national membership database, which allows him or her to use his or her membership at any of L.A. Tan's locations. To enroll, customers are required to have their fingerprints scanned. In addition, defendant discloses its customer fingerprint data to an out-of-state third-party vendor, namely, SunLync.").

139. *Id.*

140. *Id.* ¶ 9 ("Plaintiff alleges (1) that she has never been informed of the specific purposes or length of time for which defendant collected, stored or used her fingerprints, (2) that she has never been informed of any biometric data retention policy developed by defendant or whether defendant will ever permanently delete her fingerprint data, (3) that she has never been provided with nor signed a written release allowing defendant to collect or store her fingerprints, and (4) that she has never been provided with nor signed a written release allowing defendant to disclose her biometric data to SunLync to or any other third party.").

141. *Id.* ¶ 10–11 ("Plaintiff further alleges that, in 2013, more than 65% of L.A. Tan's salons were in foreclosure and that defendant's customers have not been advised what would happen to their biometric data if defendant's salon went out of business. Plaintiff alleges that she becomes emotionally upset and suffers from mental anguish when she thinks about what would happen to her biometric data if defendant went bankrupt or out of business or if defendant's franchisor, L.A. Tan, went bankrupt or out of business, or if defendant shares her biometric data with others." (footnote omitted)).

142. *Id.* ¶ 14.

143. *See* Insler, *supra* note 5, at 37 (citing Sekura v. Krishna Schaumberg Tan, Inc., No. 2016 CH 4945, 2017 WL 1181420 (Ill. Cir. Ct. Feb. 9, 2017), *rev'd*, 2018 IL App (1st) 180175).

144. *See Sekura*, 2017 WL 1181420, at *2 ("The language of BIPA itself in this respect is brief and straightforward: it provides a cause of action for 'any person aggrieved' by its violation. The most natural reading of this language alone is broad, suggesting in context that any person whose biometric data was mishandled in violation of BIPA has a claim based on such violation." (citation omitted)); *see also* Insler, *supra* note 5, at 37 (explaining that the Court found actual injury was not

meaning of "aggrieved party" by looking to precedent and its use in other statutes.[145]

In January 2018, Krishna moved the court to reconsider its ruling in light of the Second District's opinion in *Rosenbach v. Six Flags Entertainment Corp.*[146] The trial court granted the motion and reversed its earlier 2017 ruling.[147] In its order, the trial court cited "the reasons outlined in *Rosenbach v. Six Flags Entertainment Corp.*" as its motivation for dismissing Sekura's claim under BIPA.[148]

Following this decision, Sekura appealed the trial court's dismissal of her claim.[149] On September 28, 2018, the Appellate Court for the First District reversed the dismissal of Sekura's BIPA claim, finding that the trial court was correct when it originally denied Krishna's motion to dismiss in 2017.[150] The appellate court addressed the issue of standing and it held that a party did not need to show harm beyond a technical violation of the statute to be "aggrieved."[151] The court reached this

required to be aggrieved, and that a technical violation of BIPA was sufficient).

145. *See Sekura*, 2018 IL App (1st) 180175, ¶ 17 (drawing meaning for "aggrieved" by looking at other statutes and stating, "a review of other similar statutes provides further support for the broad intended reach of [the Act]. As the plaintiff points out in its supplemental brief on legislative history, both the Genetic Information Privacy Act and the AIDS Confidentiality Act provide for a substantially identical, 'any person aggrieved' right of recovery and have been interpreted as not requiring actual damages be pled." (citations omitted) (quoting *Sekura*, 2017 WL 1181420, at *2)).

146. *Id.* ¶¶ 19–20; *see, e.g.*, Neuburger, *supra* note 135 (noting that the order dismissed the claims for reasons outlined in *Rosenbach*). The holding in *Rosenbach v. Six Flags Entertainment Corp.*, 2017 IL App (2d) 170317, is discussed in note 164, *infra*.

147. *Sekura*, 2018 IL App (1st) 180175, ¶ 20 ("On January 16, 2018, the trial court granted defendant's motion to reconsider and reversed its earlier ruling. Since the order is short and it is the order being appealed from, we provide it here in full: 'This matter coming before the Court on Defendant's Motion to Reconsider and adequate notice having been given, and the Court being duly advised in the premises, IT IS HEREBY ORDERED: 1. For the reasons outlined in *Rosenbach v. Six Flags Entertainment Corp.*, Defendant's Motion is GRANTED.'" (citation omitted)); *see also* Neuburger, *supra* note 135 (discussing that the order was very brief, but referenced *Rosenbach*).

148. *Sekura*, 2018 IL App (1st) 180175, ¶¶ 19–20. *See* case discussion *infra* note 164 (discussing the two questions for review in *Rosenbach*).

149. *Id.* ¶ 21 (Defendant filed a notice of appeal on January 22, 2018); *see, e.g.*, Scott Holland, *Appeals Panel: Cook County Judge Wrong to Toss Class Action vs LA Tan Franchisee Over Customer Finger Scans*, COOK COUNTY REC. (Oct. 2, 2018), https://cookcountyrecord.com/stories/511585668-appeals-panel-cook-county-judge-wrong-to-toss-class-action-vs-la-tan-franchisee-over-customer-finger-scans (describing Sekura's appeal on January 22).

150. *Sekura*, 2018 IL App (1st) 180175, ¶ 21; Russel Perdew & Chethan Shetty, *Biometrics: Illinois Appellate Court Potentially Revives "No-Injury" Lawsuits Under the Biometric Information Privacy Act*, JD SUPRA (Oct. 5, 2018), https://www.jdsupra.com/legalnews/biometrics-illinois-appellate-court-93201/.

151. *Sekura*, 2018 IL App (1st) 180175, ¶ 84 ("First, we find that the trial court was initially correct and that, pursuant to both the plain language of the statute itself and its legislative history and purpose, the Act does not require a harm in addition to a violation of the Act in order to file suit. The Act states, very simply, that any person "aggrieved by a violation of this Act" may sue. It does *not* state that a person aggrieved by a violation of this Act—*plus* some additional harm—may

finding by using statutory interpretation.[152] The court addressed the plain meaning of "any person aggrieved by a violation of this Act" and found that it did not require additional harm *beyond* a statutory violation.[153] The court also found that legislative intent and enforcement of similar statutes in Illinois demonstrated that parties could sue for violation of BIPA without proving additional harm.[154] In its decision, the court addressed *Rosenbach* and disagreed with its sister district's interpretation of what constituted an aggrieved party within the meaning of BIPA.[155] The court also found that, even if it were to accept *Rosenbach*'s interpretation that more harm than a technical violation is necessary, Sekura satisfied the requirement because she alleged emotional injury resulting from Krishna's sharing of her data with a third party.[156]

In December 2017, Illinois's Second District Appellate Court reached a similar holding to the *McCollough* court in *Rosenbach v. Six Flags Entertainment Corp.*[157] Six Flags is an Illinois amusement park that utilized biometric scanning to identify season pass holders, and Rosenbach was the mother of a minor that visited the park.[158] Six Flags

sue." (citation omitted) (citing and interpreting 740 ILL. COMP. STAT. 14/20 (2018))).

152. *Id.* ¶ 41–42 (explaining that its goal in interpreting BIPA was "to ascertain the legislat[ors'] intent, and the best indication of their intent is the plain and ordinary meaning of the words they chose to use" and that in "interpreting a statute, we do not read a portion of it in isolation; instead, we read it in its entirety, keeping in mind the subject it addresses and the drafters' apparent objective in enacting it." (alteration in original) (quoting People v. Miles, 2017 IL App (1st) 132719, ¶ 25)); *see* Perdew & Shetty, *supra* note 150 (discussing that the lack of definition for "aggrieved party" has led to conflicting interpretations).

153. *Sekura*, 2018 IL App (1st) 180175, ¶ 50; *see also* 740 ILL. COMP. STAT. 14/20 (2018) (describing the right of action of any person aggrieved).

154. *Sekura*, 2018 IL App (1st) 180175, ¶ 57, 72 (finding that "the legislative purpose and history further supports our conclusion that plaintiff has standing to sue under the Act. . . . [O]ur review of a statute that is similar in purpose and wording to the Act at issue further supports our finding that plaintiff may sue for a violation of the Act without proving additional harm.").

155. *Id.* ¶ 74 (holding that Rosenbach's interpretation of "aggrieved" is unpersuasive) (citing Rosenbach v. Six Flags Entm't Corp., 2017 IL App (2d) 170317, ¶ 23, *rev'd*, 2019 IL 123186).

156. *Id.* ¶ 76 ("Even if we were persuaded by *Rosenbach*'s finding, we would still conclude that plaintiff's allegations in the case at bar were sufficient to support a cause of action. Unlike the plaintiff in *Rosenbach*, plaintiff in our case did allege an 'injury or adverse effect,' as *Rosenbach* required. Specifically, she alleged (1) an injury to her legal right to privacy of her own biometric information; by the disclosure of this information to an out-of-state third party vendor, and (2) mental anguish." (citation omitted) (citing *Rosenbach*, 2017 IL App (2d) 170317, ¶ 28)).

157. *See Rosenbach*, 2017 IL App (2d) 170317, ¶ 28 (holding that "If a person alleges only a technical violation of the Act without alleging any injury or adverse effect, then he or she is not aggrieved and may not recover under any of the provisions . . . ."); *see also* Insler, *supra* note 5, at 37 (explaining that the court reviewed *McCollough* in its decision and followed its reasoning).

158. *Rosenbach*, 2017 IL App (2d) 170317, ¶¶ 7–10; *see also* Radecki & Dean, *supra* note 46 ("The plaintiff alleged that Six Flags violated BIPA by collecting her minor son's fingerprints at a security checkpoint after he purchased a season pass. She claimed that Six Flags failed to provide any written information before recording her son's fingerprints and that she never consented to the collection of her son's fingerprints.").

fingerprinted the minor at a security checkpoint when he purchased a season pass and collected, recorded, and stored this data.[159] Rosenbach alleged that Six Flags violated BIPA because it did not provide written information of the specific purpose and length of time that the data would be used, failed to obtain consent for collection, storage, and use of the biometric data, and did not get a signed release regarding the fingerprint data.[160] Rosenbach did not, however, allege that Six Flags sold or mishandled her son's biometric data.[161]

Six Flags moved to dismiss, arguing that Rosenbach lacked standing because BIPA requires that a party show actual harm to be considered aggrieved.[162] The trial court denied Six Flag's motion, but later granted its motion for reconsideration and certified questions to the appellate court.[163]

The Second District Appellate Court's review focused on whether a party was "aggrieved" under BIPA when the only injury alleged was a violation of notice and consent requirements.[164] Ultimately, the court found for Six Flags, concluding that, because Rosenbach alleged only a technical violation of BIPA, she was not aggrieved and therefore did not have standing.[165] To reach its decision, the appellate court examined case

159. *Rosenbach*, 2017 IL App (2d) 170317, ¶¶ 7–10 ("When Alexander purchased his season pass, he went to the security checkpoint at the park and his thumb was scanned into the Six Flags 'biometric data capture system.' Then he went to the administrative building to obtain a season-pass card to use in conjunction with his thumbprint scan to gain access to the park."); *see also, e.g.*, Radecki & Dean, *supra* note 46; *see Private Rights of Action*, *supra* note 115 (describing when the fingerprints were collected for security purposes without obtaining consent).

160. *Rosenbach*, 2017 IL App (2d) 170317, ¶ 8 ("Plaintiff alleged that she did not consent in writing to the collection, storage, use, sale, lease, dissemination, disclosure, redisclosure, or trade of, or for Six Flags to otherwise profit from, Alexander's thumbprint 'or associated biometric identifiers or information.'"); *see also, e.g.*, Radecki & Dean, *supra* note 46 (recounting the fingerprint recordation); *see Private Rights of Action*, *supra* note 115 (noting that the fingerprints were collected without obtaining consent).

161. *See Rosenbach*, 2017 IL App (2d) 170317, ¶ 10 ("Plaintiff alleged not that she or Alexander suffered any actual injury, but that, had she known of defendants' conduct, 'she never would have purchased a season pass for her son.'"); *see also* Radecki & Dean, *supra* note 46 (explaining that plaintiff did not allege mishandling of her son's data).

162. *Rosenbach*, 2017 IL App (2d) 170317, ¶ 12.

163. *Id.* ¶¶ 15–16.

164. *See id.* ¶ 15 ("[T]he trial court . . . certified the following two questions for our review: (1) whether an individual is an aggrieved person under section 20 of the Act and may seek statutory liquidated damages . . . when the only injury he or she alleges is a violation . . . of the Act by a private entity that collected his or her biometric identifiers and/or biometric information without providing him or her the disclosures and obtaining the written consent required by . . . the Act and (2) whether an individual is an aggrieved person under section 20 of the Act and may seek injunctive relief . . . when the only injury he or she alleges is a violation . . . of the Act by a private entity that collected his or her biometric identifiers and/or biometric information without providing him or her the disclosures and obtaining the written consent required.").

165. *Id.* ¶ 28.

law and legislative intent to interpret the word "aggrieved."[166] The court found that BIPA requires plaintiffs to "allege some actual harm" instead of merely showing that a defendant failed to comply with the statutory requirements.[167] The plaintiff appealed this decision to the Illinois Supreme Court.[168]

The Illinois Supreme Court agreed to take the *Rosenbach* appeal on May 30, 2018, and heard oral arguments on November 20, 2018.[169] At oral argument, both parties focused on the word "aggrieved" and discussed the statutory construction and legislative intent of BIPA.[170] Rosenbach's counsel referred to the First District's holding in *Sekura* throughout his argument and urged the Illinois Supreme Court to reach a similar conclusion.[171] During argument, the justices raised concern regarding Six Flags's argument that actual harm was necessary to bring suit under BIPA.[172] The justices discussed BIPA's goal of preventing

166. *Id.* ¶ 23 (The Court also interpreted the legislative intent and concluded that "if the Illinois legislature intended to allow for a private cause of action for every technical violation of the Act, it could have omitted the word 'aggrieved' and stated that every violation was actionable. A determination that a technical violation of the statute is actionable would render the word 'aggrieved' superfluous.") (referencing the finding in McCollough v. Smarte Carte, Inc., No. 16 C 03777, 2016 WL 4077108 (N.D. Ill. Aug. 1, 2016)).

167. *Id.* ¶ 1; *see, e.g.*, Insler, *supra* note 5, at 37.

168. *See* Steven Grimes & Eric J. Shinabarger, *Illinois Supreme Court to Hear BIPA Standing Case*, WINSTON & STRAWN LLP: PRIVACY & DATA SECURITY L. BLOG (July 10, 2018), https://www.winston.com/en/privacy-law-corner/illinois-supreme-court-to-hear-bipa-standing-case.html (discussing the upcoming Illinois Supreme Court case); *see, e.g.*, *Fresh Rise in BIPA Lawsuits*, *supra* note 136 (discussing that Illinois Supreme court is opening the question again); Perdew & Shetty, *supra* note 150 (discussing that the plaintiff likely would appeal to the Illinois Supreme Court).

169. *E.g.*, Neuburger, *supra* note 135 (describing the *Rosenbach* decision on May 30); Winston Luo, *Rosenbach v. Six Flags: Oral Arguments Heard on Case Determining Standing Under Illinois Biometric Privacy Law*, HARV. J.L. & TECH.: JOLTDIGEST (Dec. 10, 2018), https://jolt.law.harvard.edu/digest/rosenbach-v-six-flags-oral-arguments-heard-on-case-determining-standing-under-illinois-biometric-privacy-law (noting that oral arguments were heard on November 20, 2018).

170. *See* Luo, *supra* note 169 (summarizing that the attorneys for Rosenbach argued that aggrieved means "aggrieved" means "deprived of a legal right" while the Six Flags attorneys argued that a person must be "adversely affected" or "harmed"); *see also* Gallo, *supra* note 28 (explaining that both parties looked to legislative intent and statutory construction of 740 ILL. COMP. STAT. 14/1).

171. *See* Amy Harwath, *The Fight over Standing under the Biometric Information Privacy Act Continues in Illinois High Court*, SHEPPARD MULLIN: LAB. & EMP. L. BLOG (Nov. 28, 2018), https://www.laboremploymentlawblog.com/2018/11/articles/privacy/biometric-information-privacy-act-notice-and-consent/ ("The recent *Sekura* decision played a significant role in the *Rosenbach* parties' oral arguments before the Illinois Supreme Court on November 20. During arguments, Rosenbach's counsel relied on the First District's opinion that BIPA's statutory language 'does *not* state that a person aggrieved by a violation of this act—*plus* some additional harm—may sue.'").

172. *See* Lauraann Wood, *Ill. Justices Doubt Six Flags' View in Biometric Data Case*, LAW360 (Nov. 20, 2018, 5:27 PM), https://www.law360.com/articles/1103847/ill-justices-doubt-six-flags-view-in-biometric-data-case (noting that "[a]t least three of the court's seven justices seemed

future harm and questioned whether privacy protection would be compromised if a technical violation of the statute was not sufficient to bring a claim under BIPA.[173]

On January 25, 2019, the Illinois Supreme Court handed down its decision in *Rosenbach v. Six Flags Entertainment Group*.[174] In a unanimous decision, the court held a person is "aggrieved" when there is a technical violation of BIPA; a showing of further harm is not necessary to bring a cause of action under the statute.[175]

III. ILLINOIS'S SUPREME COURT WEIGHS IN

Before the Illinois Supreme Court's decision in *Rosenbach*, the state of BIPA litigation was uncertain because of conflicting interpretations at the intermediate appellate level.[176] In one district, a party was not "aggrieved" unless it demonstrated harm beyond a statutory violation, while in another, it was sufficient for a party to merely allege a statutory violation.[177] The *Rosenbach* decision is significant because it provides clarity on standing under BIPA, is binding on Illinois and federal courts, and lowers the burden for plaintiffs bringing a suit under BIPA.[178]

The Illinois Supreme Court found that a violation of BIPA's technical requirements alone supports a cause of action under BIPA, and showing further harm is not necessary to bring a claim.[179] To reach this decision, the court analyzed the plain meaning of the statute, other Illinois statutes, Illinois precedent, and legislative intent to determine the meaning of

skeptical" of Six Flags's argument).

173. *Id.* (quoting Justice Burke as saying it was "'too late to wait' for the compromise to happen once a person's biometrics have been collected without their informed consent because at that point, 'they can't do anything about it . . . . They may never know, and you can't get your fingerprints back. It's irreparable harm.'"); *see also* Luo, *supra* note 169 (noting that punishment after an actual injury, such as an inappropriate disclosure or data breach, would be "too late"); *see also* Harwath, *supra* note 171 (quoting Judge Thomas, who stated, "If we were to . . . agree with your position on this case, . . . wouldn't that remove the incentive and urgency for entities to secure data?").

174. Rosenbach v. Six Flags Entm't Corp., 2019 IL 123186.

175. *Id.* ¶ 40; Chmielewski et al., *supra* note 30.

176. Perdew & Shetty, *supra* note 150 (explaining how "person aggrieved" was not defined in the statute, causing confusion among the courts).

177. *See* Alfred Saikali, *New Biometric Privacy Decision Creates More Risk for Companies Doing Business in Illinois*, JD SUPRA (Oct. 2, 2018), https://www.jdsupra.com/legalnews/new-biometric-privacy-decision-creates-25758/ (describing different holdings in Illinois's First and Second Districts).

178. S*ee, e.g.*, Perdew & Shetty, *supra* note 150 (describing how "person aggrieved" was not previously defined in the statute and how the decision provided clarity); *see also* Gallo, *supra* note 28 (explaining how the Supreme Court's decision will resolve a split among lower courts); Wood, *supra* note 172 ("While only Rosenbach's case is before the state high court, its ruling either way is teed up to set the standard for who can and cannot bring a lawsuit under BIPA going forward.").

179. *Rosenbach*, 2019 IL 123186, ¶ 40; *see* Chmielewski et al., *supra* note 30 (explaining the Court's holding).

"aggrieved."[180] This analysis was consistent with the methods the *McCollough*, *Sekura*, and lower *Rosenbach* courts used in their assessments.[181] The Illinois Supreme Court's decision is similar to the decision reached in *Sekura*, and upholds the intent of the Illinois legislature and essence of BIPA.[182]

A. The Plain Meaning of Aggrieved

The *Rosenbach* court first interpreted the plain meaning of BIPA's language to decide if Rosenbach had standing. In examining this language, the court held that BIPA's plain meaning did not require a showing of harm beyond a violation of the statute.[183] To reach this conclusion, the court observed that BIPA's plain language—"Any person aggrieved by a violation of this Act shall have a right of action"—did not require a showing of harm beyond a technical violation, and refused to read a more demanding standard than appeared on the face of BIPA.[184] To find BIPA required a showing of actual harm where none was listed would have required the court to disregard the plain and unambiguous language of the law.[185] The logic of the *Rosenbach* decision is simple and straightforward; Illinois precedent informs that the best indication of a drafter's intent is the plain meaning of the words chosen.[186] Because BIPA simply states "aggrieved by violation," it naturally follows the legislature intended to provide private parties with a cause of action for mere statutory violations, and the *Rosenbach* court correctly interpreted the plain language without adding superfluous language that was not

180. *Rosenbach*, 2019 IL 123186, ¶ 24; *see* Chmielewski et al., *supra* note 30 ("In reaching its decision, the court first looked to the legislative intent, explaining that the Act vests in individuals and customers the right to control their biometric data by requiring notice before collection and giving them the power to say no by withholding consent.").

181. *See, e.g.*, McCollough v. Smarte Carte, Inc., No. 16 C 03777, 2016 WL 4077108, at *4 (N.D. Ill. Aug. 1, 2016); Rosenbach v. Six Flags Entm't Corp., 2017 IL App (2d) 170317, ¶ 18, *rev'd*, 2019 IL 123186; Sekura v. Krishna Schaumburg Tan, Inc., 2018 IL App (1st) 180175, ¶ 49.

182. *See, e.g.*, *Sekura*, 2018 IL App (1st) 180175 (holding that BIPA did not require a showing of harm beyond a statutory violation).

183. *Rosenbach*, 2019 IL 123186, ¶ 40 ("Contrary to the appellate court's view, an individual need not allege some actual injury or adverse effect, beyond violation of his or her rights under the Act, in order to qualify as an 'aggrieved' person and be entitled to seek liquidated damages and injunctive relief pursuant to the Act.").

184. 740 ILL. COMP. STAT. 14/20 (2018); *Rosenbach*, 2019 IL 123186, ¶ 24.

185. *Rosenbach*, 2019 IL 123186, ¶ 38.

186. *See id.* ¶ 24 ("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." (citing Acme Markets, Inc. v. Callanan, 923 N.E.2d 718 (Ill. 2009))); *see also Sekura*, 2018 IL App (1st) 180175, ¶ 50 ("'[T]he best indication' of the drafters' intent is 'the plain and ordinary meaning of the words they chose to use.'" (citing People v. Miles, 2017 IL App (1st) 132719, ¶ 40)).

originally included.[187]

In aid of its attempt to give "any person aggrieved" its plain meaning, the *Rosenbach* court consulted the Merriam-Webster's Collegiate Dictionary and Black's Law Dictionary for a definition of the word "aggrieved."[188] Merriam-Webster defines "aggrieved" as "suffering from an infringement or denial of legal rights," and Black's Law defines it as "having legal rights that are adversely affected."[189] These definitions supported the court's ultimate conclusion that under BIPA, a party is aggrieved when his legal right was violated. Harm beyond a statutory violation is not required.

This court's interpretation of BIPA's plain meaning closely mirrors the analysis in *Sekura*.[190] First, the *Sekura* court observed that BIPA simply allows an "aggrieved party" to sue and an allegation of additional harm is not required.[191] The court held that if BIPA drafters had intended to require additional harm, they could have explicitly stated it.[192] Because the drafters did not state an additional harm requirement, the court in *Sekura* found that the plain language supported the plaintiff.[193] The *Sekura* court also consulted Black's Law Dictionary to inform its interpretation and found that BIPA gave the plaintiff "legal rights" which were "adversely affected" when the Act was violated; a showing of further harm was unnecessary.[194]

Overall, the Illinois Supreme Court's reading of BIPA's language is logical. It is consistent with the plain language of BIPA because it does not add an injury requirement where there is none, and it ultimately respects the underlying intent of the law—to protect the citizens of Illinois's sensitive biometric data.

B. Intent of the Illinois Legislature: What Is the Purpose of BIPA?

At the core of the Illinois Supreme Court's interpretation of BIPA was

187. 740 ILL. COMP. STAT. 14/20.

188. *Rosenbach*, 2019 IL 123186, ¶ 32.

189. *Id.* (citing *Aggrieved*, MERRIAM-WEBSTER'S COLLEGIATE DICTIONARY (11th ed. 2006), and *Aggrieved*, BLACK'S LAW DICTIONARY (9th ed. 2009)).

190. *Sekura*, 2018 IL App (1st) 180175.

191. *Id.* ¶ 50.

192. *Id.* ("If the drafters had intended to limit the pool of plaintiffs to those plaintiffs who had been both aggrieved by a violation of the Act *and* aggrieved by some additional harm or injury, they could have easily stated that.").

193. *Id.* (noting that the Illinois legislature "chose to state only 'a violation of this Act.' Thus, the plain language of the Act supports plaintiff's right to sue" (citation omitted)).

194. *Id.* ¶ 52 ("In other words, the Act provides plaintiff with 'legal rights' that she alleges were 'adversely affected' by the Act's violation. Defendant quotes this definition in its brief to this court, and we agree that it is persuasive. But applying the words of this definition to the facts of this case supports plaintiff's right to sue.").

an examination of the intent of the legislature.[195] By analyzing the legislature's intent, the court sought to respect and further the purpose of BIPA, and to apply the legislature's intent to inform the meaning of "aggrieved."[196] Through this analysis, the Supreme Court found that the Illinois legislature did not intend plaintiffs to have to show harm beyond a statutory violation.[197]

In exploring the intent of the legislature, this court reviewed the General Assembly's assessment of the risks posed by the growing use of biometrics by businesses.[198] In 740 ILCS 14/5, the General Assembly noted the unique and precious nature of biometric information and expressed concern over the lack of recourse an individual had if the information was compromised.[199] The court found that the Illinois legislature was particularly concerned about these risks because "[t]he full ramifications of biometric technology are not fully known."[200] Keeping this concern in mind, the court found that the legislature intended to *prevent* possible damage, not merely remedy past violations.[201] In order to accomplish this goal, the court observed that BIPA imposes strict safeguards on the collection and protection of data and subjects entities to liability regardless of whether actual damages beyond a violation of the law are shown.[202] The combination of the General Assembly's "stated purpose" and structure of the Act demonstrated to the court that the legislature meant BIPA to be a protective and deterrent law.[203] To find that BIPA required an additional showing of harm beyond a statutory violation would be "antithetical" to the purpose that the legislature envisioned.[204]

The Illinois Supreme Court's reasoning is supported by a similar finding in the *Sekura* court. The court in *Sekura* utilized legislative history and records in its interpretation of the legislature's intent to

195. Rosenbach v. Six Flags Entm't Corp., 2019 IL 123186, ¶ 35.

196. *Id.* ¶¶ 33–35 (discussing standing under BIPA and connecting it with the legislative intent of the General Assembly).

197. *Id.* ¶ 34 ("When a private entity fails to adhere to the statutory procedures, as defendants are alleged to have done here, 'the right of the individual to maintain [his or] her biometric privacy vanishes into thin air. The precise harm the Illinois legislature sought to prevent is then realized.' This is no mere 'technicality.' The injury is real and significant." (citation omitted) (quoting Patel v. Facebook, 290 F. Supp. 3d 948, 954 (N.D. Cal. 2018)).

198. *Id.* ¶ 35.

199. *See id.* (citing 740 ILL. COMP. STAT. 14/5(c)'s provision regarding the unique nature of biometric information that can result in stolen identities and other risks if compromised).

200. *Id.* (alteration in original) (citing 740 ILL. COMP. STAT. 14/5(f) (2018)).

201. *Id.* ¶ 36 (finding that the strategy of the legislature was to "head off" problems before they occurred).

202. *Id.*

203. *Id.* ¶ 37 (citing 740 ILL. COMP. STAT. 14/5).

204. *Id.*

conclude that a mere statutory violation of BIPA created an "aggrieved" person.[205] The decision described the highly sensitive, individualized nature of biometric data and reasonable fear of Illinois citizens in the collection of this data because the full ramifications of its use are unknown.[206] The court also noted that individuals were left with no recourse after their data is compromised, except to sue for damages—which are tenuous—and that the legislators enacted BIPA to prevent a compromise in the first place.[207] The court found that BIPA was intended to be proactive, rather than reactive because BIPA's "goal is to prevent irretrievable harm from happening and to put in place a process and rules to reassure an otherwise skittish public."[208] The *Sekura* court also held that forcing a member of the public to wait until after an "irretrievable harm" occurred in order to sue would "confound the very purpose of the Act."[209] As such, the court held that BIPA is not meant to provide redress only for individuals whose information has already been compromised; rather, BIPA is meant to hold companies accountable so that breaches do not occur.[210]

The Illinois Supreme Court also rebuked the holding of the lower *Rosenbach* court. The court below conducted a close reading of the statutory language to deduce the legislative intent.[211] In so doing, the lower court found that the legislature intended for the term "aggrieved" to be synonymous with "injured."[212] The court determined that "if the Illinois legislature intended to allow for a private cause of action for every technical violation of the Act, it could have omitted the word 'aggrieved'

205. Sekura v. Krishna Schaumburg Tan, Inc., 2018 IL App (1st) 180175, ¶¶ 57–58 ("While we do not find that the words were ambiguous, we do find that the legislative purpose and history further supports our conclusion that plaintiff has standing to sue under the Act. The legislative purpose is easy to discern because the legislators provided a section in the Act entitled: 'Legislative findings; intent.'" (citing 740 ILL. COMP. STAT. 14/5)).

206. *Id.* ¶¶ 62–65 ("So, we are in very serious need of protections for the citizens of Illinois when it comes to biometric information. I know of no opposition to the legislation and I'll attempt to answer any questions." (quoting H.R. Debate Transcript, 95th Gen. Assemb. No. 276, at 249 (Ill. 2008) (statement of Rep. Kathy Ryg)).

207. *Id.* ¶ 59 (citing 740 ILL. COMP. STAT. 14/5).

208. *Id.* ¶¶ 59, 64 ("Representative Ryg's remarks establish that the primary impetus behind the bill was to alleviate the fears of 'thousands of customers . . . wondering what will become of their biometric and financial data' and to provide them with protections." (omission in original) (quoting H.R. Debate Transcript, 95th Gen. Assemb. No. 276, at 249 (Ill. 2008) (statement of Rep. Kathy Ryg))).

209. *Id.* ¶ 59 (holding that Defendant's position is inconsistent with the legislature's stated goal of preventing compromise of information).

210. *See, e.g.*, *id.*

211. *See, e.g.*, McCollough v. Smarte Carte, Inc., No. 16 C 03777, 2016 WL 4077108 (N.D. Ill. Aug. 1, 2016); Rosenbach v. Six Flags Entm't Corp., 2017 IL App (2d) 170317, ¶ 23 (analyzing word choice in statute to determine legislature's intent), *rev'd*, 2019 IL 123186.

212. *Rosenbach*, 2017 IL App (2d) 170317, ¶¶ 22–23.

and stated that every violation was actionable."[213]

Essentially, the lower court found that the word "aggrieved" would be superfluous if the legislature had intended to make a technical violation actionable, and therefore, an individual who asserts a technical violation without further injury was not an aggrieved person.[214] The appellate court did not cite to the legislative history of BIPA, nor did it extrapolate on the state of privacy regulation in Illinois at the time that BIPA was enacted.[215] The court briefly mentioned the "Legislative Intent" section of BIPA, describing the Act's purpose as "to provide standards of conduct for private entities in connection with the collection and possession of biometric identifiers and biometric information."[216] But, it did not connect this section to its interpretation of "aggrieved."[217]

The Illinois Supreme Court emphatically dismissed the lower court's findings on the legislature's intent and found that the lower court's characterization of a BIPA violation as merely "technical" minimized the harm that the legislature sought to combat.[218] The right of an individual to control the use of his deeply personal biometric information is central to the purpose of BIPA, and the deprivation of this ability is the "precise harm the Illinois legislature sought to prevent."[219] As such, the Illinois Supreme Court rejected the notion that further harm needed to be demonstrated, as the injury of losing control over biometric privacy is "real and significant" by itself.[220]

The Illinois Supreme Court was correct to overturn the lower court's decision because the lower court failed to take a comprehensive view of the legislature's intent. Instead of examining the history and circumstances under which the Illinois legislature passed BIPA, the decision solely relied upon a close statutory reading to construe the intent behind the word "aggrieved."[221] The lower court's approach was

213. *Id.* ¶ 23.

214. *Id.*

215. *See id.* ¶¶ 19–23 (conducting a close reading of the language in the statute, but not conducting an examination of the atmosphere in which BIPA was created).

216. *Id.* ¶ 4 (citing 740 ILL. COMP. STAT. 14/5 (2018)).

217. *See id.* ¶ 19 (discussing the legislative intent without reference to 740 ILL. COMP. STAT. 14/5).

218. *See* Rosenbach v. Six Flags Entm't Corp., 2019 IL 123186, ¶ 34 (observing that the appellate court's finding that the violation was "merely 'technical'" misapprehends the nature of the harm our legislature is attempting to combat through this legislation).

219. *See id.* (finding that losing a right to privacy is the exact harm that the legislature sought to avoid).

220. *Id.*

221. *See Rosenbach*, 2017 IL App (2d) 170317, ¶ 23 (speculating that the word "aggrieved" would be superfluous if used to describe a statutory violation and concluding that it must therefore be synonymous to "injury").

misguided because it failed to consider the sensitive nature of biometric data, the uncertainty regarding protection of the data, and its increasing use in business. As discussed in the Illinois Senate and embodied explicitly in statutory language, BIPA was passed to protect Illinois citizens from potential breaches, and is a proactive statute, rather than a retroactive one.[222] Instead of addressing these issues, the lower court relied on less persuasive points to analyze the word "aggrieved."

The Illinois Supreme Court's reasoning is persuasive because it places high importance on the legislative intent of BIPA.[223] This evidence is important because precedent places great weight on legislative intent when conducting statutory interpretation.[224] Additionally, the legislature clearly stated its intent in the legislative reasoning section of BIPA, and the *Rosenbach* court's analysis of this section was logical and gave the legislature's intent its proper weight. The court's holding that the legislature did not intend for an "aggrieved party" to have suffered an injury beyond a statutory violation is strongly rooted in BIPA's legislative history.[225] Its decision honors the intent of the legislature and provides the intended protection of consumer information.

C. Construction of Other Illinois Statutes

In its decision, the Illinois Supreme Court also analyzed the construction of other Illinois statutes to aid its interpretation of the word "aggrieved."[226] Its review of the Consumer Fraud and Deceptive Business Practice Act and the AIDS Confidentiality Act supported the court's finding that harm beyond the violation of BIPA is not necessary

222. *See* H.R. Debate Transcript, 95th Gen. Assemb. No. 276, at 249 (Ill. 2008) (statement of Rep. Kathy Ryg) (describing the Illinois legislature's intent to protect sensitive data); *see also* 740 ILL. COMP. STAT. 14/5 (BIPA's described goal is to safeguard information).

223. 740 ILL. COMP. STAT. 14/5(c).

224. *Rosenbach*, 2017 IL App (2d) 170317, ¶ 19 ("Defendants' argument raises a question of statutory construction, which invokes well-settled principles. Our primary objective in construing a statute is to ascertain and give effect to the legislative intent, and the surest and most reliable indicator of that intent is the plain and ordinary meaning of the statutory language itself." (citing People v. Chapman, 2012 IL 111896)); *see also* Sekura v. Krishna Schaumburg Tan, Inc., 2018 IL App (1st) 180175, ¶ 42 ("'When interpreting a statute, we do not read a portion of it in isolation; instead, we read it in its entirety, keeping in mind the subject it addresses and the drafters' apparent objective in enacting it.' When considering the drafters' objective, we examine the problems that the legislature intended to remedy with the law and the consequences of construing it one way or the other." (citations omitted) (quoting People v. Miles, 2017 IL App (1st) 132719, ¶ 25)) (referencing extensive Illinois legislative history).

225. *See Sekura*, 2018 IL App (1st) 180175, ¶ 57 ("If the words of a statute are ambiguous, and only if they are ambiguous, may we turn to other aides, such as legislative history. While we do not find that the words were ambiguous, we do find that the legislative purpose and history further supports our conclusion that plaintiff has standing to sue under the Act." (citations omitted)).

226. *See* Rosenbach v. Six Flags Entm't Corp., 2019 IL 123186, ¶¶ 25–26 (citing 815 ILL. COMP. STAT. 505/10a(a) (2018), and 410 ILL. COMP. STAT. 305 (2018)).

to be "aggrieved."[227]

The court first examined the Consumer Fraud and Deceptive Business Practice Act.[228] In this statute, the language plainly states that in order to bring a claim, an aggrieved party must suffer *actual* damage beyond a violation.[229] The *Rosenbach* court interpreted this to mean that when the Illinois legislature intends to require such a showing of damages, it makes that intention clear.[230] Because BIPA does not contain such language, the court found that the drafters did not intend to require damage beyond a statutory violation.[231] Contrarily, Illinois's AIDS Confidentiality Act does not provide any requirement for actual harm beyond a statutory violation.[232] It offers a private right of action for a party "aggrieved" by a violation of the statute but does not define "aggrieved."[233] In *Doe v. Chand*, the Fifth District Appellate Court found that proof of actual damages was not required to recover under the statute.[234] The *Rosenbach* court viewed the Fifth District's interpretation of the AIDS Confidentiality Act as "instructive" to its interpretation of the similarly worded standing language in BIPA.[235] Comparing the AIDS Confidentiality Act to BIPA aided in the *Rosenbach* court's decision that a plaintiff is not required to show harm beyond a statutory violation.

The *Sekura* court also conducted a comparison of BIPA to the AIDS Confidentiality Act. The *Sekura* court's analysis differed slightly, but ultimately it reached a similar decision to the court in *Rosenbach*. In *Sekura*, the court noted two important similarities between BIPA and the AIDS Confidentiality Act.[236] First, the AIDS Confidentiality Act employs similar "right of action" statutory language to BIPA, including the offering of a right of action to "[a]ny person aggrieved by a

227. *Id.*

228. *Id.* ¶ 25 (citing 815 ILL. COMP. STAT. 505/10a(a)).

229. *Id.* (citing 815 ILL. COMP. STAT. 505/10a(a), which states that "[a]ny person who suffers actual damage as a result of a violation of this Act committed by any other person may bring an action against such person." This statute requires damage beyond a violation of a statute.).

230. *Id.* ("When the General Assembly has wanted to impose such a requirement in other situations, it has made that intention clear.").

231. *Id.* ¶ 26 (referencing 410 ILL. COMP. STAT. 305).

232. *Id.* (citing 410 ILL. COMP. STAT. 305/13).

233. *Id.* ¶ 29 (comparing BIPA by stating, "As with the AIDS Confidentiality Act, the Act does not contain its own definition of what it means to be 'aggrieved' by a violation of the law.").

234. *Id.* ¶ 26 (citing Doe v. Chand, 781 N.E.2d 340, 351 (Ill. App. Ct. 2002), which found that proof of actual damages is not required to recover).

235. *Id.* ¶ 28 (noting that the Fifth Circuit's decision is not "dispositive," but nonetheless provided support for the Supreme Court's opinion).

236. *See* Sekura v. Krishna Schaumburg Tan, Inc., 2018 IL App (1st) 180175, ¶ 68 (comparing 740 ILL. COMP. STAT. 14/20 to the AIDS Confidentiality Act by stating, "Of the various statutes, the closest one for comparison's sake is the AIDS Confidentiality Act.").

violation."[237] Second, the court in *Sekura* found that the purposes of the AIDS Confidentiality Act and BIPA were similar.[238] The court determined the legislative purpose of the AIDS Confidentiality Act was to "relieve the fears of people about being tested for AIDS and to protect against unauthorized disclosure."[239] The *Sekura* court held that BIPA's purpose was similar because its intent was to relieve the fears of using and relying on new technology and to protect against unauthorized disclosure.[240] Because of the similarities between the AIDS Confidentiality Act and BIPA in both statutory language and purpose, the court in *Sekura* applied the "aggrieved party" definition under the AIDS Confidentiality Act to BIPA and held that a technical violation created an aggrieved party under both.[241]

The comparison of BIPA to the AIDS Confidentiality Act is logical due to the similarities in language and overall purpose. Under Illinois law, courts can turn to other codes when such codes have similar goals and subjects.[242] The *Rosenbach* court's careful comparison provided a strong reference point.

D. Illinois Case Law

This *Rosenbach* court also found support for its holding in Illinois Supreme Court precedent.[243] Specifically, the court analyzed prior interpretations of the word "aggrieved."[244] These cases supported the

---

237. *Id.* ¶ 69 (alteration in original). The court stated as follows:

> Both sections provide recovery against a person who "negligently violates a provision of this Act" or "intentionally or recklessly violates a provision of this Act." Both provide for liquidated or actual damages, "whichever is greater." Both sections provide for reasonable attorney fees, as well as "other relief, including an injunction."

Id. (citations omitted) (citing 740 ILL. COMP. STAT. 14/20 (2018), and 410 ILL. COMP. STAT. 305/13).

238. *See id.* ¶ 70 (comparing 740 ILL. COMP. STAT. 14/5, and 410 ILL. COMP. STAT. 305/2 and stating, "In addition, the two statutes have similar purposes.").

239. *Id.* (referencing 410 ILL. COMP. STAT. 305/2(2)).

240. *Id.* ("In both situations, disclosure can create irreparable harm.").

241. *Id.* ¶ 72 ("Thus, our review of a statute that is similar in purpose and wording to the Act at issue further supports our finding that plaintiff may sue for a violation of the Act without proving additional harm.").

242. *Id.* ¶ 67 ("[W]hile we may turn to other codes, we should only do so when the codes share similar goals and related subjects . . . [A] statute should be 'construed in conjunction with other statutes touching on the same or related subjects' 'considering the reason and necessity for the law, the evils to be remedied, and the objects and purposes to be obtained.'" (first alteration in original) (quoting Maschek v. City of Chicago, 2015 IL App (1st) 150520, ¶ 71)).

243. Rosenbach v. Six Flags Entm't Corp., 2019 IL 123186, ¶¶ 30–31 (citing Glos v. People, 102 N.E. 763 (Ill. 1913); Am. Surety Co. v. Jones, 51 N.E.2d 122 (Ill. 1943); *In re* Estate of Hinshaw, 153 N.E.2d 422 (Ill. App. Ct. 1958); *In re* Estate of Harmston, 295 N.E.2d 66 (Ill. App. Ct. 1973); Greeling v. Abendroth, 813 N.E.2d 768 (Ill. App. Ct. 2004)).

244. *Id.* ¶ 30.

finding that the violation of a statute without further harm can create an aggrieved party.[245] Illinois precedent informs that a party can be aggrieved when they suffer a denial of a personal or property right.[246] A person who suffers actual damages as the result of a violation of his rights would meet this definition, but sustaining such damages is not necessary to qualify as "aggrieved."[247] Rather, Illinois courts look to see if a person's legal rights have been invaded.[248] This meaning of the term "aggrieved" is "embedded" in Illinois jurisprudence, and the Illinois Supreme Court was not persuaded to find otherwise.[249] Additionally, the court concluded that this definition is so well settled in Illinois law that the authors of BIPA must have known of the precedent and intended for the word "aggrieved" to have such meaning.[250]

These references are more helpful than the analysis conducted by the lower *Rosenbach* court. The lower court relied on two federal district court cases, *McCollough v. Smarte Carte, Inc.* and *Vigil v. Take-Two Interactive Software, Inc.*, that found a technical violation did not create standing under BIPA.[251] Although federal court opinions interpreting state law are not binding on Illinois courts, the court in *Rosenbach* found their analyses to be persuasive.[252] The Illinois Supreme Court, on the other hand, correctly placed greater weight on Illinois precedent, making for a more relevant and convincing analysis and holding.[253] The meaning of BIPA's "aggrieved party" provision is best informed by the state of the

245. *Id.*

246. *Id.* (citing *Glos*, 102 N.E. at 766 and stating that "[a] person is prejudiced or aggrieved, in the legal sense, when a legal right is invaded by the act complained of or his pecuniary interest is directly affected by the decree or judgment.").

247. *Id.* ("A person who suffers actual damages as the result of the violation of his or her rights would meet this definition of course, but sustaining such damages is not necessary to qualify as 'aggrieved.'").

248. *Id.*

249. *Id.* ¶ 31 (finding that this understanding of "aggrieved" has been used frequently by Illinois courts).

250. *Id.* ("We must presume that the legislature was aware of that precedent and acted accordingly." (citing People v. Cole, 2017 IL 120997, ¶ 30, which observed that "when statutes are enacted after judicial opinions are published, it must be presumed that the legislature acted with knowledge of the prevailing case law")).

251. *See* Rosenbach v. Six Flags Entm't Corp., 2017 IL App (2d) 170317, ¶ 21 (stating that in *McCollough*, "the plaintiff sought damages stemming from violations of the Act. . . . [T]he district court held that, by alleging a technical violation of the Act, the plaintiff did not meet that definition, because she had not alleged any facts to show that her rights had been adversely affected by the violation." (citing McCollough v. Smarte Carte, Inc., No. 16 C 03777, 2016 WL 4077108, at *4 (N.D. Ill. Aug. 1, 2016))), *rev'd*, 2019 IL 123186; *see also id.* (citing Vigil v. Take-Two Interactive Software, Inc., 235 F. Supp. 3d 499, 519–20 (S.D.N.Y. 2017)).

252. *See id.* ("While cases from lower federal courts are not binding, we may consider their analyses persuasive.").

253. *See Rosenbach*, 2019 IL 123186, ¶ 31 (citing five Illinois cases as it assessed how to interpret the meaning of "aggrieved").

law in Illinois at the time the Act was passed. The fact that "aggrieved" had a commonly known definition at the time of passage strongly suggests that the legislature created the statute with this definition in mind.[254] Additionally, the court followed the precedent of Illinois state courts rather than following the nonbinding decisions of federal courts.[255]

Overall, the *Rosenbach* decision is sound as it closely follows Illinois precedent and reflects the Illinois legislature's intent to protect consumers proactively rather than retroactively. The court recognized that the Illinois legislature intended to protect the information of its citizens, and the court conducted analysis that was consistent with Illinois rules of statutory construction to find that a technical violation of BIPA creates an aggrieved party.

IV. IMPACTS OF THE *ROSENBACH* DECISION

On January 25, 2019, the Illinois Supreme Court handed down its decision in *Rosenbach v. Six Flags Entertainment Corp.*[256] This decision resolved the inter-district split over whether a person must allege an injury beyond a procedural violation of BIPA in order to be "aggrieved."[257] The Illinois Supreme Court ultimately found in favor of a generous grant of standing to those that allege a mere technical violation rather than the more onerous showing of actual injury. The *Rosenbach* decision will have a significant impact on litigation and enforcement of BIPA in both Illinois state and federal courts across the country.[258] The low standing threshold of an "aggrieved party" will also affect businesses that employ the use of biometric technology, as they will need to ensure that they are in compliance with the statute or else face serious liability from individual and class action litigation.[259] Additionally, Illinois may

254. *Id.* (stating that "[w]e must presume that the legislature was aware of that precedent and acted accordingly") (citing *Cole*, 2017 IL 120997, ¶ 30).

255. The lower *Rosenbach* court cited *McCollough*, 2016 WL 4077108, and *Vigil*, 235 F. Supp. 3d 499, both of which were federal cases.

256. *Rosenbach*, 2019 IL 123186.

257. *Id.* ¶ 40 (holding that "an individual need not allege some actual injury or adverse effect, beyond violation of his or her rights under the Act, in order to qualify as an 'aggrieved' person and be entitled to seek liquidated damages and injunctive relief pursuant to the Act.").

258. *See, e.g.*, Perdew & Shetty, *supra* note 150 (discussing the implications of the decision); *see also* Cynthia J. Larose & Elana Safner, *No Harm, Still a Foul: Illinois Supreme Court Rules on the Collection of Biometric Data*, NAT'L L. REV. (Jan. 29, 2019), https://www.natlawreview.com/article/no-harm-still-foul-illinois-supreme-court-rules-collection-biometric-data (observing that this ruling will have a large impact on future litigation and will create a "boon" for plaintiffs); Mira Baylson et al., *Rosenbach v. Six Flags - Illinois Supreme Court Takes Expansive View of Statutory Standing Under the Biometric Information Privacy Act*, JD SUPRA (Jan. 29, 2019), https://www.jdsupra.com/legalnews/rosenbach-v-six-flags-illinois-supreme-86315/ (finding that this decision will likely increase the amount of lawsuits under BIPA).

259. *See* Ambrose McCall, *Following Supreme Court Decision, It's High Time for Illinois*

soon be joined by other states who seek to implement measures similar to BIPA as there is growing awareness of the importance of biometric privacy. Lastly, this decision is a major victory for consumers because it offers the most robust protection of their sensitive data as well as substantive recourse when their privacy rights are violated.

A. The Effect on Litigation

The Illinois Supreme Court's decision will have a major impact on litigation under BIPA because the low standing threshold will inevitably lead to an increase in the types and number of claims that are brought.[260] Opponents of *Rosenbach* reasonably fear that a wave of frivolous lawsuits will follow this decision.[261] However, this decision will also positively impact future litigation by providing clarity on the matter of standing.

Those opposed to the *Rosenbach* decision fear it will lead to a chaotic increase in class action suits or a potential floodgate in litigation.[262] Critics argue that Illinois will become a "gotcha" state, in which potential plaintiffs actively seek to catch potential offenders in procedural mistakes.[263] This is a valid concern; the private right of action coupled

---

Employers to Review Workplace Biometric Privacy Issues, JD SUPRA (Jan. 30, 2019), https://www.jdsupra.com/legalnews/following-supreme-court-decision-it-s-20018/ (stating that in light of this recent decision, there is heightened importance for employers to comply with BIPA); *see also* Jeff John Roberts, *Court's Biometrics Ruling Poses Billion Dollar Risk to Facebook, Google*, FORTUNE (Jan. 28, 2019), http://fortune.com/2019/01/28/facebook-face-scanning-bipa/ (noting that companies that violate BIPA could be subject to "enormous" fines if involved in class actions).

260. *See* Larose & Safner, *supra* note 258 ("More than 100 businesses accused of violating BIPA have closely watched the case, and it is likely the ruling may embolden plaintiffs' attorneys to add to the over 200 BIPA cases brought in Illinois state courts. Many of these cases were stayed in anticipation of the Rosenbach decision."); s*ee also* Allison Grande, *Ill. Biometric Ruling a Boon to Plaintiffs, Yet Questions Linger*, LAW360 (Jan. 25, 2019, 10:14 PM), https://www.law360.com/articles/1122234/ill-biometric-ruling-a-boon-to-plaintiffs-yet-questions-linger ("The recent influx of litigation under Illinois' unique Biometric Information Privacy Act is set to intensify . . . .").

261. *See* Grande, *supra* note 260 ("The ruling is expected to embolden plaintiffs' attorneys to continue to pad a BIPA docket that already exceeds 200 cases . . . ."); *see also* Baylson et al., *supra* note 258 (observing that this could lead to many more suits filed even if such suits do not claim an alleged loss).

262. *See* Perdew & Shetty, *supra* note 150 (describing a wave of class action litigation); *see also* Brief of Amicus Curiae Illinois Chamber of Commerce in Support of Defendant-Appellees Six Flags Entertainment Corporation and Great America LLC at 4, Rosenbach v. Six Flags Entm't Corp., 2017 IL App (2d) 170317 (No. SC123186), 2018 WL 5777926 ("Reversal of the Appellate Court's decision will open the floodgates for future litigation at the expense of Illinois' commercial health.").

263. *See* Grande, *supra* note 260 (citing one commentator who remarked, "With their ruling today, the Illinois Supreme Court has decided that BIPA is a 'gotcha' statute, and if businesses don't use the magic words when using biometric technology, then they're going to be looking at hundreds of thousands to millions of dollars in exposure."); *see also* Roberts, *supra* note 259 (observing that companies could lose billions in a major class action suit).

with a smaller hurdle for plaintiff's attorneys—who are entitled to fees and costs if victorious—will undoubtedly attract more litigation.[264]

However, the *Rosenbach* decision provides the necessary clarity to lower Illinois courts that were split over the "aggrieved party" provision of BIPA.[265] The *Rosenbach* holding provides lower courts with a bright-line standing requirement, which will avoid squandering judicial resources on lengthy procedural motions. Parties doing business in Illinois or with Illinois citizens are now fully aware that in order to collect and keep biometric data, they must be fully compliant with BIPA's technical requirements governing retention, collection, disclosure, and destruction of such data, otherwise they face significant liability.[266] Prior to *Rosenbach*, the courts struggled to come to a clear answer on which types of injury were sufficient to grant standing under BIPA, and grappled with where to draw the line on standing.[267] The lack of clarity and its consequences were evident in *Sekura*.[268] Although *Sekura* found that a showing of injury beyond statutory violation was unnecessary, the *Sekura* court still observed that the plaintiff had suffered an actual injury.[269] The court found that the plaintiff's "mental anguish" and the sharing of data to a third-party vendor constituted an adverse effect, which can be grounds to find someone an "aggrieved party."[270] However, legal commentators observed that emotional harm was likely insufficient to show actual injury under BIPA.[271] Moving forward, there will be less

264. *See* Chmielewski et al., *supra* note 30 (surmising that this ruling will come as "welcome news to plaintiffs' attorneys" because there are now "fewer impediments to pursue no-injury class action lawsuits under BIPA"); *see also* Grande, *supra* note 260 (observing that one plaintiff's firm is planning to resume forty-five cases it had stayed while waiting for the court to decide this case).

265. *See* Larose & Safner, *supra* note 258 (stating that the meaning of aggrieved is finally settled); *see also* Michael McGivney et al., *Biometrics: Illinois Supreme Court Allows No-Injury Biometric Information Privacy Act Claims in Complete Victory for Plaintiffs' Bar*, JD SUPRA (Jan. 28, 2019), https://www.jdsupra.com/legalnews/biometrics-illinois-supreme-court-86872/ ("The Supreme Court in *Rosenbach* gave a clear and final answer that will be binding on all courts that consider BIPA claims: plaintiffs need only allege a statutory violation to have a private right of action and an ability to collect statutory damages.").

266. *See* Chmielewski et al., *supra* note 30 (observing that there has been uncertainty on the interpretation of BIPA, but this ruling establishes clear procedures that a business must adopt in order to remain compliant).

267. *See* Sekura v. Krishna Schaumburg Tan, Inc., 2018 IL App (1st) 180175, ¶ 85 (determining that Plaintiff alleged an actual injury).

268. *Id.*

269. *Id.* ¶ 76 ("Unlike the plaintiff in *Rosenbach*, plaintiff in our case did allege an 'injury or adverse effect' . . . .").

270. *Id.* ¶ 85 ("[D]isclosure to an out-of-state third-party vendor constitutes an injury or adverse effect, and plaintiff in the instant case alleged such a disclosure, while the *Rosenbach* plaintiff did not. Second, the mental anguish that plaintiff alleges in her complaint also constitutes an injury or adverse effect." (citation omitted)).

271. *See* Saikali, *supra* note 177 (suggesting that only compromise of data in a hacking would be an injury); *see also Illinois Appellate Court Restricts BIPA Claims*, MICHAEL BEST (Jan. 4,

scenarios like the one seen in *Sekura*, because the Illinois Supreme Court was clear and unanimous in its decision. This decision does not answer all questions about BIPA, but it does provide much-needed clarity.[272]

B. Business Considerations

The Illinois Supreme Court did consider the effect that its holding on standing under BIPA would have on businesses that must comply with the Act.[273] Critics of *Rosenbach* argue that by doing away with an actual injury requirement, BIPA lawsuits will significantly harm businesses and technological innovation in Illinois.[274] This fear is reasonable; the combination of a lower showing of harm, private right of action, award of damages per violation, and reasonable attorneys' fees and costs poses serious liability to any business that operates in Illinois or simply has customers in the state.[275] Business advocates suggest that companies will be forced to do a costly risk assessment to determine if they can accept the potential liability of implementing new and innovative technologies that use customers' biometric data in Illinois.[276]

It is true that *Rosenbach* makes Illinois unique in its level of protection of consumers' biometric data; however, there is no indication that this decision's interpretation of what it means for a party to be aggrieved will compromise businesses' ability to compete with other states.[277] Of

---

2018), https://www.michaelbest.com/Newsroom/159002/Illinois-Appellate-Court-Restricts-BIPA-Claims (speculating that answer of emotional harm is not settled).

272. *See* Grande, *supra* note 260 ("[G]iven the wealth of outstanding legal issues that remain to be litigated under the statute, the question of which side will have the upper hand in these disputes in the future is far from settled."); *see also* Chmielewski et al., *supra* note 30 ("Questions remain as to the applicability of BIPA in many fields, and how entities may operate so as to ensure compliance with same in such instances of uncertainty.").

273. Rosenbach v. Six Flags Entm't Corp., 2019 IL 123186, ¶ 37.

274. *See* Saikali, *supra* note 177 (commenting on high litigation costs); note 94, *supra*.

275. *See* Roberts, *supra* note 259 (observing that companies could lose billions in a major class action suit); *see also* Grande, *supra* note 260 ("The Supreme Court's answer to the certified question of what the statute means by 'aggrieved' is poised to not only restart the scores of litigation that has been put on hold in anticipation of the Rosenbach decision, but also clear the way for more plaintiffs seeking to recoup uncapped statutory damages of between $1,000 and $5,000 per violation to at least make it through the courthouse doors.").

276. *See* Grande, *supra* note 260 (quoting a commentator who felt that the ruling "really opened a can of worms and declared open season on a lot of legitimate businesses that are trying to be innovative"); *see also* Baylson et al., *supra* note 258 (discussing that businesses will have to do a cost-benefit analysis to see if it makes economic sense to use new technologies).

277. In fact, the technology industry in Illinois has continued to grow after the enactment of BIPA. *See* Ill. Sci. & Tech. Coal., *Illinois' Share of High-Tech Businesses is Among the Nation's Top States*, CHI. TRIB. (Oct. 15, 2014, 11:00 AM), https://www.chicagotribune.com/bluesky/hub/chi-iin-illinois-high-tech-businesses-bsi-hub-story.html (describing growth of the technology industry in Illinois); Mark Schultz, *The Illinois Economy Kicks Off 2018 With Strong Numbers*, ILL. PUB. MEDIA NEWS (Feb. 5, 2018), https://will.illinois.edu/news/story/the-illinois-economy-kicks-off-2018-with-strong-numbers (same).

course, it would not be in Illinois's best interest to set impossible standards of compliance for companies and hinder business operations. However, BIPA does not impose such unworkable standards. Businesses should not fear a statutory violation because the standards for retention, collection, disclosure, and destruction of biometric data under BIPA are fair and achievable.[278] In addition to being easy to implement, it is also less costly for companies to implement smart data protection policies that monitor compliance with biometric laws in the first instance than to respond to a massive breach of consumers' protected biometric data.[279] It is in the best interest of both businesses and consumers to implement a robust biometric protection policy that prevents data compromises and the ensuing liability.[280]

Companies that use biometric data can continue their practices; they simply must ensure their policies conform to BIPA's modest consent and disclosure requirements.[281] Illinois businesses and out-of-state businesses with Illinois users or customers should implement policies regarding the handling of sensitive biometric data so that they are compliant with BIPA.[282] In general, companies should implement robust

278. *See* Kay, *supra* note 13, at 3 ("[T]he general requirements for compliance are relatively straightforward: biometric identifiers and information cannot be sold and cannot be kept longer than the shorter of three years or until the original purpose for which they were collected is satisfied, and companies should implement and adhere to robust written policies and procedures for collecting and safeguarding biometric identifiers and information, and obtain written consent from the persons from whom they were obtained in order to use them.").

279. Rosenbach v. Six Flags Entm't Corp., 2019 IL 123186, ¶ 37 ("Compliance should not be difficult; whatever expenses a business might incur to meet the law's requirements are likely to be insignificant compared to the substantial and irreversible harm that could result if biometric identifiers and information are not properly safeguarded . . . ."); *see also* note 63, *supra*.

280. The costs of data breaches are increasing. *See IBM Study: Hidden Costs of Data Breaches Increase Expenses for Businesses*, IBM NEWS ROOM (July 11, 2018), https://newsroom.ibm.com/2018-07-10-IBM-Study-Hidden-Costs-of-Data-Breaches-Increase-Expenses-for-Businesses (finding that "the average cost of a data breach globally is $3.86 million," which represents an increase of 6.4 percent from 2017); *see also* Niall McCarthy, *The Average Cost of a Data Breach Is Highest in the U.S.*, FORBES (July 13, 2018, 7:30 AM), https://www.forbes.com/sites/niallmccarthy/2018/07/13/the-average-cost-of-a-data-breach-is-highest-in-the-u-s-infographic/#4bb575592f37 (finding that the average cost of a data breach in the United States is $7.9 million, which is the highest in the world).

281. *See* Michael J. Bologna, *Biometric Privacy Ruling Boosts Cases Against Companies*, BLOOMBERG L.: BIG L. BUS. (Jan. 25, 2019), https://biglawbusiness.com/biometric-privacy-ruling-boosts-cases-against-companies-corrected (quoting a Chicago law firm partner that stated the ruling would "encourage companies to take reasonable and entirely non-burdensome steps to ensure biometrics are protected"); *see also* McCall, *supra* note 259 (suggesting that employers conduct privacy audits to make sure that their policies are compliant with this statute).

282. *See* Zielinksi, *supra* note 9 ("'It's essential to also have a written policy in place.' . . . 'The policy should detail exactly the type of devices being used and what specifically they're being used for. That should be clear so employees can't later claim they didn't know how and why biometrics would be used in the workplace.'"); *see also A New Threat from an Old Source*, *supra* note 16 (providing programs for employers so that they are compliant with BIPA standards); Kay, *supra*

written policies and procedures for collecting and safeguarding biometric information, should always provide written notice to their users, and get written consent that provides the intended use of the biometric data. Additionally, companies should avoid selling any information or keeping the data for over three years, and develop a plan for destruction of the material. If businesses develop a compliant plan and adhere to the straightforward guidelines of BIPA, standing based on a statutory violation will not be harmful. In any event, as the *Rosenbach* court noted, "[W]hatever expenses a business might incur to meet the law's requirements are likely to be insignificant compared to the substantial and irreversible harm that could result if biometric identifiers and information are not properly safeguarded."[283]

C. The Expansion of Privacy Laws

The *Rosenbach* decision reflects a trend of growing concern regarding data privacy and is likely a preview of future state and federal legislation ahead. Although Illinois currently has the most stringent biometric collection policy, other states may soon join Illinois in offering stronger protection for biometric information.[284] In June 2018, California's governor signed the California Consumer Protection Act (CCPA).[285] This act establishes a broad privacy framework that businesses must

note 13 (same).

283. Rosenbach v. Six Flags Entm't Corp., 2019 IL 123186, ¶ 37.

284. *See* David Cohen, Nicholas Farnsworth & Aravind Swaminathan, *Roller Coaster Start to the New Year for Biometrics: Rosenbach v. Six Flags and Emerging Biometric Laws*, JD SUPRA (Feb. 15, 2019), https://www.jdsupra.com/legalnews/roller-coaster-start-to-the-new-year-90991/ (observing that California, Washington, Massachusetts, and New York are considering implementation of new privacy statutes); Andrew C. Glass, Gregory N. Blase & Daniel S. Cohen, *Massachusetts State Senators Seek to Enact Biometric Data Protection Law*, NAT'L L. REV. (Feb. 11, 2019), https://www.natlawreview.com/article/massachusetts-state-senators-seek-to-enact-biometric-data-protection-law ("In Massachusetts, for instance, four state senators introduced a bill (S.D 341) in late January that would require companies to refrain from collecting personal and biometric data absent express consent from the affected consumer."); Odia Kagan, *Multiple States Considering New Data Privacy Legislation*, FOX ROTHSCHILD (Feb. 10, 2019), https://dataprivacy.foxrothschild.com/2019/02/articles/california-consumer-privacy-act/multiple-states-considering-new-data-privacy-legislation/ (stating that data privacy bills are pending in at least eight states); Andreas Kaltsounis & Shea Leitch, *Washington State Proposes Sweeping Privacy Legislation*, JD SUPRA (Feb. 5, 2019), https://www.jdsupra.com/legalnews/washington-state-proposes-sweeping-95926/ (describing a new Washington privacy law that was proposed in January 2019).

285. Shoshana S. Speiser, *Recent Developments in California Privacy Law*, MANATT (Sept. 13, 2018), https://www.manatt.com/Insights/Newsletters/Advertising-Law/Recent-Developments-in-California-Privacy-Law (note that amendment passed later); *see Your Readiness Roadmap for the California Consumer Privacy Act (CCPA)*, PWC, https://www.pwc.com/us/en/services/consulting/cybersecurity/california-consumer-privacy-act.html (last visited June 18, 2019) (The CCPA will go into effect in 2020).

follow and provides consumers greater control of their data.[286] Some notable provisions of this act include an expanded definition of "personal information," creating new rights for California consumers to control their data, imposing new rules on the collection of personal information from minors, and creating a private right of action for some statutory violations.[287]

Similarly, the state of Washington is considering a proposed law, the Washington Privacy Act (WPA), which would create a set of consumer rights similar to those provided in CCPA.[288] In Massachusetts, state senators introduced a bill[289] in late January that would require companies to refrain from collecting personal and biometric data absent express consent from the affected consumer.[290] Like BIPA and CCPA, this Act would also provide a private right of action.[291] Lastly, the state of New York is considering the enactment of its own biometric privacy act.[292] The proposed act would be similar to BIPA, providing individuals a private right of action if they were aggrieved by any violation of the

286. *See* Cohen, Farnsworth & Swaminathan, *supra* note 284 ("The CCPA introduced sweeping changes to the U.S. privacy landscape by granting California residents enhanced rights in relation to their personal information (which includes biometric information), as well as a private right of action for certain breaches of personal information.").

287. *See id.* (explaining the details of the CCPA and noting that personal information includes biometric privacy); *see also* Harry A. Valetk & Brian Hengesbaugh, *A Practical Guide to CCPA Readiness: Implementing Calif.'s New Privacy Law (Part 1)*, CORP. COUNS. (Dec. 10, 2018, 10:40 AM), https://www.law.com/corpcounsel/2018/12/10/a-practical-guide-to-ccpa-readiness-implementing-calif-s-new-privacy-law-part-1/?slreturn=20190116174958 (discussing changes from the CCPA).

288. *See* Kaltsounis & Leitch, *supra* note 284 (explaining that the new statute requires that companies provide consumers with access, deletion, correction, restriction, portability, objection, and protections from profiling); *see also* Cohen, Farnsworth & Swaminathan, *supra* note 284 (noting similarities between the Washington Privacy Act and the CCPA).

289. S. 120, 191st Gen. Court (Mass. 2019).

290. *See* Glass, Blase & Cohen, *supra* note 284 (describing that the bill "would require companies to refrain from collecting personal and biometric data absent express consent from the affected consumer. . . . [and] consumers could request a copy of their personal data that has been collected, restrict disclosure of their data to third parties, and even require the business to delete their data"); *see also* Cohen, Farnsworth & Swaminathan, *supra* note 284 (describing the Massachusetts bill which grants consumers rights in relation to personal information).

291. *See* Glass, Blase & Cohen, *supra* note 284 ("The bill also contemplates granting consumers a private right of action to obtain the greater of actual damages or $750 per incident, injunctive or declaratory relief, and reasonable attorneys' fees. Notably, the bill would expressly confer standing to sue regardless of whether the unauthorized biometric data collected caused actual harm"); Cohen, Farnsworth & Swaminathan, *supra* note 284.

292. *See* Stephanie J. Kapinos, *New York City Considers Facial Recognition Bill—Will New York Be the Next Forum for Biometric Privacy Litigation?*, NAT'L L. REV. (Jan. 31, 2019), https://www.natlawreview.com/article/new-york-city-considers-facial-recognition-bill-will-new-york-be-next-forum (explaining that New York City Council members introduced a bill (Bill Int. No. 1170) for the city council that would regulate the use of biometric technology).

statute.[293]

These enacted and proposed laws demonstrate a growing recognition of the importance of biometric privacy protection.[294] Illinois was at the forefront of implementing biometric privacy protections, but action in state legislatures across the county reflect a growing concern for data privacy. In addition to protections at the state level, the federal government appears poised to consider implementing uniform data protection regulation in the near future.[295] Consumers, data privacy advocates, and technology companies alike have voiced support for a consistent federal privacy policy.[296] Between new state statutes and a possible federal law, it is likely that the protection of data will be an important topic for years to come. Illinois, through BIPA, has offered a strong template for future data protection legislation.

---

293. *See id.* (noting that the statute requires businesses to give notice to customers if they are collecting "biometric identifier information." The bill "includes a private right of enforcement but avoids the statutory standing issue litigated in *Rosenbach* by providing that 'any person who[se] biometric identifier information was collected, retained, converted, stored or shared in violation of [the law] may commence an action.'" (alteration in original)).

294. *See* Glass, Blase & Cohen, *supra* note 284 ("The growing use of Big Data and biometric data has caused some concern among consumers and policymakers. In response, several state legislatures have taken steps to regulate companies' ability to acquire personal and biometric data."); Kagan, *supra* note 284.

295. *See* Grande, *supra* note 260 (predicting that less stringent federal laws may be advocated for by the business community); *see also* Dan Clark, *Federal Data Privacy Legislation Is Likely Next Year, Tech Lawyers Say*, CORP. COUNS. (Nov. 29, 2018, 5:00 PM), https://www.law.com/corpcounsel/2018/11/29/federal-data-privacy-legislation-is-likely-next-year-tech-lawyers-say/ (surmising that 2019 may be a year that a federal statute is proposed as "[m]ore and more people have become aware of how much of their personal information is on the internet, and they are more aware of the risks of having that information exposed. Over the past couple of months, legislators, trade organizations and even tech companies have stepped up their efforts to pass data privacy and cybersecurity legislation"). S*ee also* David Meyer, *In the Wake of GDPR, Will the U.S. Embrace Data Privacy?*, FORTUNE (Nov. 29, 2018), http://fortune.com/2018/11/29/federal-data-privacy-law/ (discussing the impact that the EU's General Data Protection Regulation (GDPR) may have on US policy). The GDPR provides greater privacy protection for consumers as it mandates consent and gives consumers more control over their data (for instance, they can delete information after they provide it). *Id.* The act imposes large fines on those that violate the regulation. US Companies who work in the EU have to comply with this statue. *Id.* This statute provides unity and greater consumer protection, and some advocates would like the U.S. to follow suit. *Id.*

296. *See* Tony Romm, *Can Washington Keep Watch over Silicon Valley? The FTC's Facebook Probe Is a High-Stakes Test*, WASH. POST (Feb. 20, 2019), https://www.washingtonpost.com/technology/2019/02/20/can-washington-keep-watch-over-silicon-valley-ftcs-facebook-probe-is-high-stakes-test/?noredirect=on&utm_term=.566ea863c581 (commenting on the desire for a uniform federal law as some privacy advocates have found that the lack of uniformity in data protection results in inconsistent enforcement); *see also* Danielle Abril, *This Is What Tech Companies Want in Any Federal Data Privacy Legislation*, FORTUNE (Feb. 21, 2019), http://fortune.com/2019/02/21/technology-companies-federal-data-privacy-law/ ("Several big technology companies have a message for any U.S. lawmakers crafting new data privacy rules: Follow our advice." Technology companies are lobbying for a uniform law because complying with "hodgepodge" state laws is burdensome and these companies hope to provide guidance on provisions in this possible statute.).

Until more states and possibly the federal government take their own action to protect sensitive consumer data, BIPA, as interpreted by *Rosenbach*, will likely have significant extraterritorial reach. Illinois is the sixth most populous state, and Chicago is home to some of the world's largest technology companies and a burgeoning tech startup community.[297]

In short, any company, technology or otherwise, that wishes to do business in Illinois, or with Illinois users, will have to comply with BIPA. While companies could segregate Illinois customers and users into their own more robust data privacy protocol, this seems unlikely and cost inefficient. More likely is that businesses subject to BIPA will adopt BIPA-compliant data privacy policies for *all* its customers and users, regardless of state citizenship.[298]

D. Protection of Consumers

The Illinois Supreme Court's *Rosenbach* decision recognized the

297. *See* Benjamin Elisha Sawe, *The 50 US States Ranked By Population*, WORLDATLAS, https://www.worldatlas.com/articles/us-states-by-population.html (last updated Sept. 14, 2018) (listing populations of states); *see also* Conor Cawley, *15 Fastest Growing Tech Companies in Chicago*, TECH.CO (Dec. 13, 2017, 9:20 AM), https://tech.co/news/fastest-growing-tech-companies-chicago-2017-12 (describing fast-growing tech companies and start-ups in Chicago); Anna Marie Kukec, *Tech Companies Are Choosing Chicago*, U.S. NEWS (Sept. 20, 2018, 12:01 AM), https://www.usnews.com/news/best-states/articles/2018-09-20/why-tech-companies-are-choosing-chicago (detailing tech companies that have expanded into Chicago, including Facebook, LinkedIn, Uber, Yelp, Google, and Microsoft).

298. For instance, Indeed, Google, and Facebook have already been subject to suit under the BIPA for their facial recognition software, and in light of *Rosenbach*, it would appear their potential liability is significant enough to cause them consider BIPA-compliant policies for all users. *See* Susan Fahringer et al., *Google Defeats Biometric Privacy Lawsuit on Article III Standing Grounds*, PERKINS COIE (Jan. 2, 2018), https://www.perkinscoie.com/en/news-insights/google-defeats-biometric-privacy-lawsuit-on-article-iii-standing-grounds.html (detailing Google's BIPA suit); Ally Marotti, *Facebook Could Be Forced to Pay Billions of Dollars Over Alleged Violations of Illinois Biometrics Law*, CHI. TRIB. (Apr. 17, 2018, 4:20 PM), https://www.chicagotribune.com/business/ct-biz-facebook-tagging-privacy-lawsuit-20180417-story.html (describing the biometric suit that Facebook was involved in); Joel Rosenblatt, *Facebook Can't Avoid Privacy Suit Over Biometric Face Prints*, BLOOMBERG: TECH. (Feb. 26, 2018, 2:26 PM), https://www.bloomberg.com/news/articles/2018-02-26/facebook-can-t-avoid-privacy-lawsuit-over-biometric-face-prints (providing information on Facebook biometric suit); *see also* Robert Fallah, *Illinois Supreme Court's Biometric Privacy Ruling Raises Liability Risk*, SHRM: ST. & LOC. UPDATES (Feb. 14, 2019), https://www.shrm.org/resourcesandtools/legal-and-compliance/state-and-local-updates/pages/illinois-supreme-court-biometric-privacy-ruling-raises-liability-risk.aspx ("At present, the issue of standing at the federal level remains unresolved, but employers would be well advised to adopt procedures similar to those required under BIPA, as more states are considering or have already introduced similar legislation and others have expanded expectations for employers to protect employees' biometric data."); Ryan S. Higgins et al., *Biometric Privacy Update – Actual Harm Not Required*, MCDERMOTT WILL & EMERY (Feb. 7, 2019), https://www.mwe.com/insights/biometric-privacy-update-actual-harm-not-required/ (suggesting that organizations closely scrutinize their biometric practices to comply with BIPA).

legislature's intent in the creation of BIPA and prioritized the protection of consumers.[299] The court found that the legislature intended for a statutory violation to create an "aggrieved party."[300] The Illinois Supreme Court's decision respected the intent of the legislature and offers heighted privacy security for consumers.

BIPA was created in response to both the growing use of biometrics and uncertainty surrounding the technology.[301] The Illinois legislature was concerned with protecting consumer data, and recognized that regulation was necessary as businesses increasingly utilized, and profited from, biometrics in Illinois.[302] Since BIPA was enacted in 2008, the use of biometric data has significantly increased and is utilized in a variety of applications and industries, and its use will only become more prevalent.[303] The widespread use of biometrics has heightened the importance of regulating the collection and use of biometric data.[304] In enacting BIPA, the Illinois legislature recognized the significance of an individual having notice and control over their data.[305] Notice ensures that individuals know how and why their information is being used, and allows individuals to make an informed decision on whether to disclose that information. Without this notice, an individual may have no way of knowing whether their information is being collected and what it is being

299. The Illinois Supreme Court utilized Illinois rules of interpretation to reach its holding that a statutory violation constitutes an aggrieved party. *See* Rosenbach v. Six Flags Entm't Corp., 2019 IL 123186, ¶¶ 33–35 (discussing standing under BIPA and connecting it with the legislative intent of the General Assembly).

300. *See id.* ¶ 34 ("When a private entity fails to adhere to the statutory procedures, as defendants are alleged to have done here, 'the right of the individual to maintain [his or] her biometric privacy vanishes into thin air. The precise harm the Illinois legislature sought to prevent is then realized.' This is no mere 'technicality.' The injury is real and significant." (citation omitted) (quoting Patel v. Facebook, 290 F. Supp. 3d 948, 954 (N.D. Cal. 2018))).

301. *See* 740 ILL. COMP. STAT. 14/5 (2018) (noting the purpose of the BIPA); *see also* Brief of Amici Curiae the American Civil Liberties Union et al. in Support of Plaintiff-Appellant at 3, Rosenbach v. Six Flags Entm't Corp., 2017 IL App (2d) 170317 (No. 123186), 2018 WL 5777921 (describing the purpose of the BIPA).

302. *See generally, e.g.*, H.R. Debate Transcript, 95th Gen. Assemb. No. 276, at 249 (Ill. 2008) (statement of Rep. Kathy Ryg) (debating the costs and benefits of the BIPA); *see also* 740 ILL. COMP. STAT. 14/5 (discussing the legislative findings and intent).

303. *See* McCray, *supra* note 2, at 77; *What Is Biometrics?*, *supra* note 6; *see also* Zielinksi, *supra* note 9.

304. *See* Brief of Amici Curiae The American Civil Liberties Union et al. in Support of Plaintiff-Appellant, *supra* note 301, at 3 ("The ensuing decade has confirmed the wisdom and necessity of the legislature's action, as the collection and use of biometric information has proliferated and the privacy threats of nonconsensual collection and use of biometric information have become even clearer.").

305. *See id.* at 9 ("Individuals cannot have a meaningful opportunity to decide whether they wish their biometric identifiers to be collected unless they have an enforceable right to notice of the 'specific purpose . . . for which . . . [the data] is being collected, stored, and used,' and to deny consent for its 'disclos[ure or] redisclos[ure].'" (alterations in original) (citation omitted) (quoting 740 ILL. COMP. STAT. 14/15)).

used for—precisely the harm that the Illinois legislature wanted to ameliorate.[306] Through BIPA's notice and consent requirement, the Illinois legislature afforded protections for individuals as soon as their data is collected rather than after a data compromise occurs.[307]

The Illinois Supreme Court's holding honors the intent of the Illinois legislature and offers strong protection for consumers. Employees, consumers, and other individuals can be confident that their information is safe and have a meaningful remedy if it is not.[308] BIPA's private right of action, with a minimal standing requirement, holds companies accountable for the unique biometric data collected, and potential liability gives a company strong incentive to comply with the commonsense requirements of BIPA.[309] Had the court in *Rosenbach* required plaintiffs show actual harm, BIPA's notice and consent requirements would have lacked enforcement power and the effectiveness of BIPA's protection would be undercut. For these reasons, the Illinois Supreme Court's decision will bolster consumer protection.

CONCLUSION

Technological innovation creates positive opportunities for Illinois companies and consumers alike. Biometrics is an emerging area of technology, and its uses and applications are only starting to be seen. In the business setting, the use of biometrics has increased convenience, security, and the ability to monitor employees. Its increasingly widespread use is a testament to its utility. However, widespread use of biometric technology carries significant risks. An individual's biometric information is highly personal and sensitive; it cannot be changed like a credit card number. Because of this, individuals have a strong interest in ensuring that their unique information is used only in the manner they intend and that the companies in possession of their data do so in a secure

306. *See id.* at 11 ("Notice is the 'most fundamental principle' of privacy protection." (quoting FED. TRADE COMM'N, PRIVACY ONLINE: A REPORT TO CONGRESS 7 (1998), https://www.ftc.gov/sites/default/files/documents/reports/privacy-online-report-congress/priv-23a.pdf)).

307. *See* H.R. Debate Transcript, 95th Gen. Assemb. No. 276, at 249 (Ill. 2008) (statement of Rep. Kathy Ryg) (discussing the BIPA's benefit to consumers).

308. Standing requires no further harm than a statutory violation.

309. *See* Grande, *supra* note 260 (describing the opinions of some commentators that found that the BIPA holding "is a profound victory for workers and consumers across Illinois who can now seek monetary damages against corporations that skirt the law and jeopardize the security of individuals' biometric data").

> When private entities face liability for failure to comply with the law's requirements without requiring affected individuals or customers to show some injury beyond violation of their statutory rights, those entities have the strongest possible incentive to conform to the law and prevent problems before they occur and cannot be undone.

Rosenbach v. Six Flags Entm't Corp., 2019 IL 123186, ¶ 37.

manner. For these reasons, the Illinois legislature passed BIPA as a means to facilitate the use of biometric data with robust protections for consumers. The legislature recognized the importance of ensuring that consumers are aware of how their data was being used and safeguarding this data to prevent harm to the individual and unauthorized transfers to third parties.

BIPA's requirements are well tailored to achieve this goal. The requirements that businesses receive informed written consent, maintain proper safeguarding regulations, have retention and destruction guidelines, and abstain from profiting from biometric data are straightforward and achieve the legislature's goals. BIPA's private right of action provision holds companies accountable for their compliance with the Act and ensures that consumers' interests are respected. The court in *McCollough* and the lower *Rosenbach* court limited the protection of individuals by requiring harm beyond a mere statutory violation as a requisite for standing. The legislature and statute intended for a consumer to be informed and protected as a means to guard against harm. To require an individual to wait until harm has occurred would frustrate the purpose of the statute.

As such, the Illinois Supreme Court was correct to overturn the lower court's decision and find that an individual is "aggrieved" when a statutory violation occurs. Its decision was logical because it followed Illinois's rules on statutory interpretation and honored the legislature's intent. Although the court's holding may increase the number of suits filed, it will also provide clarity to the legislative landscape. In light of the holding, businesses need to create clear notice and consent policies before collecting biometric data. The Illinois Supreme Court's decision is not likely to halt biometric progress, but it will augment the protection of consumers in the evolving landscape of technological developments.