Loyola of Los Angeles
Entertainment Law Review

Volume 40 | Number 1 Article 2

Fall 12-4-2019

Actual Harm Means it is too Late: How Rosenbach v. Six Flags Demonstrates Effective Biometric Information Privacy Law

Chloe Stepney
chloe.stepney@lls.edu

ACTUAL HARM MEANS IT IS TOO LATE: HOW *ROSENBACH V. SIX FLAGS* DEMONSTRATES EFFECTIVE BIOMETRIC INFORMATION PRIVACY LAW

*Chloe Stepney**

Technology is rapidly advancing, and the law is trying to keep up. While this challenge is not new, technological advancements are impacting privacy rights in unprecedented ways. Using a fingerprint to clock in at work or face identification to unlock a smartphone provides ease and convenience, but at what cost?

Currently, there is no federal law that regulates the collection, use, and storage of biometric information in the private sector. On a local level, three states have enacted laws that specifically address biometrics. Of those, the Biometric Information Privacy Act (BIPA) in Illinois provides the strongest protections for consumers, who are entitled to a private right of action under the statute. Since the enactment of BIPA about a decade ago, hundreds of plaintiffs have brought legal action against companies operating in Illinois.

This Comment explains how the Illinois Supreme Court properly applied the state's biometric information privacy statute and why the ruling in *Rosenbach v. Six Flags* should be a model for analyzing biometric information privacy rights. Part II will provide a brief history of privacy law in the United States and how the ubiquitous collection and use of biometric information threatens privacy rights. Next, Part III will describe the facts, issue, and holding of *Rosenbach v. Six Flags*. Part IV will analyze the court's examination of statutory language and legislative intent and explain how those findings lay the foundation for future regulation of biometric information. Finally, this Comment will conclude with a recommendation for legislators to rely on *Rosenbach* as an example of how biometric privacy regulation should apply in states and, one day, nationwide.

---

*J.D. Candidate, Class of 2020, Loyola Law School, Los Angeles. The author would like to thank Professor Gary Craig for his feedback, guidance, and support, and the *Loyola of Los Angeles Entertainment Law Review* editorial staff for their assistance with this article. She also wishes to give a special thank you to Ronal and Jeanne Stepney, Cesalie Stepney, and Pedro Moura for their endless love and encouragement.

I. INTRODUCTION

Type "biometric" into Google and more than forty million search results will appear in about half of a second.[1] Those results include definitions, the U.S. Department of Homeland Security website, and relevant businesses, such as security firms and nearby fingerprinting services.[2]

Click over to the "Google News" tab, and there are numerous headlines about the use of biometrics across the globe. In India, the world's largest biometric information database continues to be scrutinized.[3] In Australia, a man won a lawsuit for unjust termination after he refused to use his fingerprint to clock in and out of work.[4] In Kenya, controversy surrounds the government's rollout of a national database that stores the biometric information of its citizens.[5] In the United Kingdom, a watchdog organization demanded that a government agency delete approximately five million voiceprints collected from its citizens without proper consent.[6]

---

1. *Search: Biometric*, GOOGLE, https://www.google.com/search?source=hp&ei=uZfpXN-vIOMH_-gSY66boBw&q=biometric&oq=biometric&gs_l=psy-ab.12..0l10.588.1831..2020. . .0.0..0.112.703.8j1. . .. . .0. . ..1..gws-wiz. . . . .0..0i131.wXVXDz2pkRc [https://perma.cc/FGT3-LAK3].

2. *Id.*

3. Vindu Goel, *India's Top Court Limits Sweep of Biometric ID Program*, N.Y. TIMES (Sept. 26, 2018), https://www.nytimes.com/2018/09/26/technology/india-id-aadhaar-supreme-court.html [https://perma.cc/5222-9XN6]; *What is Aadhaar*, AADHAAR, https://uidai.gov.in/what-is-aadhaar.html [https://perma.cc/LH69-9RTA].

4. Rosie Perper, *An Australian Worker Won a Landmark Privacy Case Against His Employer After He Was Fired for Refusing to Use a Fingerprint Scanner*, BUS. INSIDER (May 22, 2019, 6:14 AM), https://www.businessinsider.com/australian-worker-wins-privacy-case-against-employer-biometric-data-2019-5 [https://perma.cc/ZK4C-PTNU].

5. Keren Weitzberg, *Kenya's Controversial Biometric Project Is Shrouded in Secrecy*, CODA STORY (May 3, 2019), https://codastory.com/authoritarian-tech/kenya-biometric-project-shrouded-in-secrecy/ [https://perma.cc/QUZ2-8CPV].

6. Natasha Lomas, *UK Tax Office Ordered to Delete Millions of Unlawful Biometric Voiceprints*, TECHCRUNCH (May 10, 2019), https://techcrunch.com/2019/05/10/uk-tax-office-ordered-to-delete-millions-of-unlawful-biometric-voiceprints/ [https://perma.cc/4Y8K-47EY].

What do all of these headlines have in common? Biometrics. The term "biometrics" describes a person's unique physiological and behavioral characteristics.[7] Physical biometric identifiers include fingerprints, hand geometry, retinas, and facial features.[8] Behavioral biometric identifiers include a person's voice, signature, and keystroke.[9] These unique identifiers can be used to conveniently and efficiently verify a person's identity.[10] For example, in the public sector, governments and law enforcement agencies collect and use biometrics for border control and cybersecurity.[11] In the private sector, employees use biometrics to track their time and access buildings.[12] Consumers use biometrics to unlock smartphones, log into mobile apps, and complete financial transactions.[13]

In the United States, where the government has managed a national database of fingerprints since 1924, the scope of biometric information is expanding.[14] For example, Amazon patented technology that would allow Alexa, Amazon's virtual assistant, to analyze sounds in a user's voice that

7. *See Definition of Biometrics*, MERRIAM-WEBSTER, https://www.merriam-webster.com/dictionary/biometrics [http://perma.cc/4LW6-ZF6G]; *What is Biometrics?*, 360 BIOMETRICS, http://www.360biometrics.com/faq/biometrics.php [https://perma.cc/RM2N-GWTF].

8. *What is Biometrics?*, *supra* note 7.

9. *Id.*

10. *Identity is at the Heart of the Digital Age*, INT'L BIOMETRICS + IDENTITY ASS'N, https://www.ibia.org/biometrics-and-identity [https://perma.cc/7SYB-QKWK].

11. *Common Applications*, INT'L BIOMETRICS + IDENTITY ASS'N, https://www.ibia.org/biometrics-and-identity/common-application [http://perma.cc/8CM9-5Q66].

12. *Id.*

13. *Id.*

14. *Fingerprints and Other Biometrics*, FED. BUREAU OF INVESTIGATION, https://www.fbi.gov/services/cjis/fingerprints-and-other-biometrics [https://perma.cc/6HBE-AKUB].

indicate sleepiness or a sore throat.[15] Then, Alexa could place an online order for cough drops or recommend eating chicken noodle soup for dinner.[16] Another patent that pushes the boundaries of biometrics belongs to Walmart.[17] The retail giant submitted a patent application for technology that would monitor a customer's body temperature and heart rate through the handle bar of a shopping cart.[18] With that data, Walmart could know when to send an employee to assist a customer who might be feeling stressed while shopping in the store.[19]

As businesses innovate, consumers are adopting biometric technology with the use of thumbprints and face identification. In a recent consumer survey, nearly half of smartphone users said they use biometric authentication to unlock their phone or to use an app on their phone.[20] Among smartphone owners who use their phone for financial activities, 63% said they use biometric authentication.[21] While this technology provides ease and efficiency, it also generates concerns regarding privacy and data security. Who owns the data? Where is biometric data stored and for how long? What

---

15. Betsy Mikel, *Amazon Quietly Just Patented a Technology to Give Alexa an Eerie Superpower*, INC. (Oct 15, 2018), https://www.inc.com/betsy-mikel/amazon-quietly-just-patented-an-eerie-technology-alexas-superpowers-are-getting-more-personal-intimate.html [https://perma.cc/Y5FR-55FD]; U.S. Patent No. 10,096,319 (issued Oct. 9, 2018); Kim Wetzel, *What Is Alexa, and What Can Amazon's Virtual Assistant Do for You?*, DIGITAL TRENDS (Feb. 16, 2019), https://www.digitaltrends.com/home/what-is-amazons-alexa-and-what-can-it-do/ [https://perma.cc/A34B-FM4U].

16. Mikel, *supra* note 15. *See also* Adam Clark Estes, *Amazon Is Getting Closer to Building an Alexa Wearable That Knows When You're Depressed*, GIZMODO (May 23, 2019, 11:20 AM), https://gizmodo.com/amazon-is-getting-closer-to-building-a-wearable-that-kn-1834973513 [https://perma.cc/2QQB-378R].

17. Betsy Mikel, *Walmart Just Filed for a Weird Patent. Shopping Carts May Never Be the Same*, INC. (Oct. 9, 2018), https://www.inc.com/betsy-mikel/walmart-just-made-an-announcement-that-may-make-you-never-want-to-shop-there-again.html [https://perma.cc/9SMG-FF3K] [hereinafter *Walmart Shopping Cart Patent*]; U.S. Patent Application 15/902,091 (filed Feb. 22, 2018).

18. *Walmart Shopping Cart Patent*, *supra* note 17.

19. *Id.*

20. Shashank Srivastava, *Biometric Authentication Is Gaining Trust – But Is It Foolproof?*, DELOITTE (Apr. 3, 2019), https://www2.deloitte.com/us/en/pages/technology-media-and-telecommunications/articles/biometric-authentication-future-applications.html [https://perma.cc/K4WJ-E6MS].

21. *Id.*

are a consumer's rights to that data? What happens if a hacker accesses a company's database of biometric information? What are the consequences of having one's fingerprint compromised?

In Illinois, a mother sued the amusement park Six Flags after her teenage son used his fingerprint to enter the park with a newly acquired season pass.[22] Plaintiff Stacy Rosenbach, on behalf of her son, alleged that Six Flags violated the Illinois Biometric Information Privacy Act (BIPA), a law enacted in 2008 to regulate the "collection, use, safeguarding, handling, storage, retention, and destruction of biometric identifiers and information," such as fingerprints.[23] In direct violation of BIPA, Six Flags allegedly failed to obtain consent or provide any information about the fingerprinting process.[24] While Six Flags did not contest those facts, it argued that a BIPA violation, by itself, is not enough to bring a lawsuit under the statute.[25] The plaintiff must sustain an actual physical, pecuniary, or emotional injury in order to have sufficient standing to bring a cause of action under BIPA.[26] The Illinois Supreme Court, however, disagreed.[27] Based on a thorough analysis of statutory construction, the court in *Rosenbach v. Six Flags* found that a person who experiences a violation of their biometric information privacy rights *is* harmed and can sue under BIPA. "[N]o additional consequences need be pleaded or proved. The violation, in itself, is sufficient to support the individual's or customer's statutory cause of action."[28] Accordingly, Rosenbach won the case, which has come to serve as a warning to businesses collecting biometric information from consumers in Illinois.[29]

---

22. Rosenbach v. Six Flags Entm't Corp., 129 N.E.3d 1197, 1200–01 (Ill. 2019).

23. *Id.* at 1201; Biometric Information Privacy Act, 740 ILL. COMP. STAT. § 14/15 (2008).

24. *Rosenbach*, 129 N.E.3d at 1200–01.

25. *Id.* at 1204.

26. *Id.*; *see also* Brief for Defendants-Appellees, Rosenbach v. Six Flags Entm't Corp., 2017 IL App (2d) 170317 (No. 123186).

27. *Rosenbach*, 129 N.E.3d at 1204.

28. *Id.* at 1206.

29. Nathan Freed Wessler, *Ruling Is a Warning to Companies Collecting Biometric Scans Without Permission*, AM. CIV. LIBERTIES UNION (Feb. 8, 2019, 4:45 PM), https://www.aclu.org/blog/privacy-technology/surveillance-technologies/ruling-warning-companies-collecting-biometric. [https://perma.cc/R4W8-CPGW]; Geeta Malhortra et al., *In Landmark Case, Illinois Supreme Court Sets Low Bar For Claims Under Illinois' Biometric Information Privacy Act, Sidley Austin: Data Matters*, SIDLEY (Jan. 31, 2019), https://datamatters.sidley.com/in-

This Comment explains how the Illinois Supreme Court properly applied the state's biometric information privacy statute and why the ruling in *Rosenbach v. Six Flags* should be a model for biometric information privacy regulation nationwide. Part II will provide a brief history of privacy law in the United States and how the ubiquitous collection and use of biometric information threatens privacy rights. Part III will describe the facts, legal issues, and holding of *Rosenbach v. Six Flags*. Part IV will discuss the court's examination of statutory language and legislative intent and explain how those findings lay the foundation for future regulation of biometric information. Finally, this Comment will conclude with a recommendation for legislators to rely on *Rosenbach* as an example of how biometric privacy law should operate in states and, one day, nationwide.

II. BACKGROUND: A PATCHWORK OF PRIVACY PROTECTION

A. Privacy Law in the United States

The rapid evolution of technology has altered the concept and scope of privacy today. In a world where people share their lives on the Internet and readily disclose personal information through mobile devices, there is an ever-present concern about privacy and the security of personal information. And that concern is increasing.[30] In a survey of adult consumers in the United States, 67% of respondents said they think the government should do more to protect data privacy, 73% would like the right to ask an organization how their data is being used, and 38% said they now use social media less often because of data privacy concerns.[31]

In the United States, legislators have taken a sectoral approach to the regulation of privacy.[32] General privacy regulations are not commonplace.

---

landmark-case-illinois-supreme-court-sets-low-bar-for-claims-under-illinois-biometric-information-privacy-act/ [https://perma.cc/KQ7K-T4MD].

30. *SAS Survey: 67 Percent of US Consumers Think Government Should Do More to Protect Data Privacy*, SAS (Dec 10, 2018), https://www.sas.com/en_us/news/press-releases/2018/december/data-management-data-privacy-survey.html [https://perma.cc/33PJ-TZPJ].

31. *Id.*

32. *See generally* Hannah Zimmerman, *The Data of You: Regulating Private Industry's Collection of Biometric Information*, 66 KAN. L. REV. 637, 644–45 (2018).

Instead, privacy standards are established for specific industries and situations.[33] For example, the Cable Communications Policy Act regulates the privacy of cable subscribers, and the Children's Online Privacy Protection Act regulates the collection of personal information from children online.[34]

This is in stark contrast to the European Union, where the General Data Protection Regulation (GDPR) took effect in May 2018.[35] The GDPR established broad protection for the personal data of European residents.[36] The law, which provided the first major update to European data protection law in over twenty years, applies to both companies based in the European Union and companies abroad that offer goods or services to people in the European Union.[37] Individual privacy rights are at the heart of the GDPR, and companies must comply with the law's principles of fairness, transparency, accuracy, and security.[38] Ultimately, European residents can now access and control their data in ways much of the world cannot.[39]

These fundamental principles of access, control, and transparency are unfamiliar to companies and consumers in the United States. On a federal level, the privacy rights of consumers are scattered across numerous laws without an overarching standard for protection and regulation.[40] As a result,

---

33. *Id.* (In the United States, "data privacy protection is limited to specific types of information in limited circumstances.").

34. *Cable Television*, FED. COMM. COMMISSION, https://www.fcc.gov/media/engineering/cable-television [https://perma.cc/8U2F-RAZR]; *Children's Privacy*, FED. TRADE COMMISSION, https://www.ftc.gov/tips-advice/business-center/privacy-and-security/children%27s-privacy [http://perma.cc/MB6N-48VJ].

35. *General Data Protection Regulation Overview*, IT GOVERNANCE, https://www.itgovernance.co.uk/data-protection-dpa-and-eu-data-protection-regulation [https://perma.cc/5FVM-PU4R].

36. *Id.*

37. *Id.*

38. *Id.*

39. Arielle Pardes, *What is GDPR and Why Should You Care?*, WIRED (May 24, 2018, 6:00 AM), https://www.wired.com/story/how-gdpr-affects-you/ [https://perma.cc/342M-R92E] ("GDPR represents one of the most robust data privacy laws in the world. It also gives [European citizens] the right to ask companies how their personal data is collected and stored, how it's being used, and request that personal data be deleted. It also requires that companies clearly explain how your data is stored and used, and get your consent before collecting it.").

40. Zimmerman, *supra* note 33, at 638; *see also* Pardes, *supra* note 39, at 2–3 ("The United States has historically regulated privacy in context, with piecemeal laws for the privacy of

consumers are unsure what rights they have, if any, and businesses are vulnerable to violations of numerous laws they may be unfamiliar with.[41] The country's siloed approach to privacy stifles the privacy rights of consumers, and consequently data protection and security.[42]

B. Protecting Biometric Information

As governments and businesses collect biometrics, those unique identifiers can be paired with other personal information, such as a name, date of birth, and social security number, making databases more robust.[43] But these large databases are vulnerable to hacks and the unauthorized sharing of data.[44] Privacy advocates warn that the collection, use, and storage of biometrics comes with extreme risks.[45] Yet, the level of risk is unclear to the public because information about how entities use, manage, and secure biometric databases is sparse.[46]

Simultaneously, the business of biometrics is booming. According to a market research report, the value of the biometrics systems market totaled $16.8 billion in 2018, with single-factor authentication, such as a fingerprint or face scan, occupying a large share of the market.[47] By 2023, the market is expected to reach $41.8 billion.[48]

---

healthcare records, financial documents, and federal communications. There's nothing analogous to GDPR in the United States, and likely won't be any time soon.").

41. Zimmerman, *supra* note 33, at 650.

42. *Id.* at 644.

43. *Biometrics*, ELECTRONIC FRONTIER FOUND., https://www.eff.org/issues/biometrics [https://perma.cc/4VKU-PWGZ].

44. *Id.*

45. *Id.*

46. *Biometrics*, AM. CIV. LIBERTIES UNION, https://www.aclu.org/issues/privacy-technology/surveillance-technologies/biometrics [https://perma.cc/5758-MFKQ].

47. Shelly Singh, Markets and Markets, *Biometrics System Mkt. Worth $41.80 billion by 2023*, PR NEWSWIRE (July 31, 2018), https://www.prnewswire.com/news-releases/biometrics-system-market-worth-41-80-billion-by-2023-805517780.html [https://perma.cc/4RN3-YB9G].

48. *Id.*

As the use of biometrics increases, the cost for businesses to use biometric technology decreases.[49] Biometric authentication can decrease operational costs because the technology provides efficiency and reduces fraud.[50] In addition to convenience, biometrics provide security,[51] a separate but related concept to privacy.[52] Unlike a traditional password that can be shared or forged, biometrics are unique characteristics that strengthen identity verification.[53]

C. Regulating the Private Sector's Collection of Biometric Information

Currently, there is no federal law that regulates the collection or use of biometric information.[54] On the state level, only three states have passed laws that specifically address the collection, use, sharing, and storage of biometric information.[55] The first of the three was Illinois, which enacted the Biometric Information Privacy Act (BIPA) in 2008 and became the first state to regulate the private sector's collection and use of biometric identifiers and information.[56] Shortly after, Texas passed the Capture or Use Biometric

49. *Biometrics + Identity*, INT'L BIOMETRICS + IDENTITY ASS'N, https://www.ibia.org/biometrics-and-identity/faqs [https://perma.cc/4Q4X-5SR6].

50. *Id.*

51. *Id.*

52. *About the IAPP*, INT'L ASS'N OF PRIVACY PROF., https://iapp.org/about/what-is-privacy/ [https://perma.cc/EN3E-85KA]. (Data privacy relates to one's rights and expectations regarding personal information, including the collecting, use, and sharing of that information. On the other hand, security *protects* that information.).

53. *Biometrics + Identity*, *supra* note 50.

54. Michael A. Rivera, *Face Off: An Examination of State Biometric Privacy Statutes & Data Harm Remedies*, 26 FORDHAM INTELL. PROP. MEDIA & ENT. L. J. 571, 576 (2019) ("Because of biometrics' relative novelty, there are currently no federal laws that specifically address the responsibilities of businesses collecting, using, or releasing biometric data.").

55. Lara Tumeh, *Washington's New Biometric Privacy Statute and How It Compares to Illinois and Texas Law*, JD SUPRA (Oct. 20, 2017), https://www.jdsupra.com/legalnews/washington-s-new-biometric-privacy-70894/ [https://perma.cc/9JA3-3KD2].

56. Biometric Information Privacy Act, 740 ILL. COMP. STAT. § 14/15 (2008).

Identifier Act (CUBI) in 2009.[57] Most recently, Washington passed a biometric privacy law in 2017.[58] In the latter two states, only the attorney general can bring legal action against a violator of the biometric law.[59] This means that Illinois is currently the only state where consumers can bring legal action against a company for a violation of their biometric information privacy rights.[60]

Section 20 of BIPA provides that "[a]ny person aggrieved by a violation of this Act shall have a right of action in a State circuit court or as a supplemental claim in federal district court against an offending party."[61] This private right of action provides plaintiffs with an opportunity to hold businesses operating in Illinois accountable in a way that is currently unavailable in all other states.[62] For example, in *McCollough v. Smarte Carte, Inc.*, a customer of Smarte Carte, a company that operated electronic storage lockers in Chicago's Union Station, sued the company for collecting, storing, and using her fingerprint without her consent.[63] In *Monroy v. Shutterfly, Inc.*, a user of Shutterfly, a digital photography website, alleged that Shutterfly unlawfully used and stored his face geometry in violation of BIPA.[64]

The private right of action, combined with the increased use of technology that employs biometrics, resulted in an uptick of BIPA litigation in both state and federal court starting around 2015.[65] To date, plaintiffs have

57. Capture or Use Biometric Identifier Act, 11 TEX. BUS. & COM. CODE § 503.001 (2009).

58. Washington Biometric Privacy Act, 19 WASH. REV. CODE § 19.375 (2017).

59. Tumeh, *supra* note 56.

60. *Id.*

61. COMP. STAT. § 14/20.

62. Tumeh, *supra* note 56.

63. McCollough v. Smarte Carte, Inc., No. 16 C 03777, 2016 WL 4077108, at *1–2 (N.D. Ill. Aug. 1, 2016).

64. Monroy v. Shutterfly, Inc., No. 16 C 10984, 2017 WL 4099846, at *1 (N.D. Ill. Sept. 15, 2017).

65. *See* Tumeh, *supra* note 56; Charles N. Insler, *Understanding the Biometric Information Privacy Act Litigation Explosion*, 106 ILL. B.J. 34, 35 (2018).

filed more than 200 cases alleging BIPA violations.[66] With more businesses implementing facial recognition and biometric scans for authenticating customers and tracking employees, putative class action lawsuits have increased.[67]

Under BIPA, a "biometric identifier" includes "a retina or iris scan, fingerprint, voiceprint, or scan of hand or face geometry."[68] The statute further clarifies that "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" are not biometric identifiers.[69] In a broader sense, "biometric information" is "any information, regardless of how it is captured, converted, stored, or shared, based on an individual's biometric identifier used to identify an individual."[70]

Any business that collects, uses, or stores biometrics in Illinois must adhere to BIPA's notice, consent, and data management requirements.[71] In addition to requiring a written policy regarding biometrics,[72] BIPA provides that:

> No private entity may collect, capture, purchase, receive through trade, or otherwise obtain a person's or a customer's biometric identifier or information, unless it first:
> (1) informs the subject . . . in writing that a biometric identifier or biometric information is being collected or stored;
> (2) informs the subject . . . in writing of the specific purpose and length of term for which a biometric identifier or biometric information is being collected, stored, and used; and

66. Kathryn E. Deal et al., *Rosenbach v. Six Flags – Illinois Supreme Court Takes Expansive View of Statutory Standing Under the Biometric Information Privacy Act*, 31 INTELL. PROP. & TECH. L.J. 17, 18 (2019).

67. *Id.*

68. Biometric Information Privacy Act, 740 ILL. COMP. STAT. § 14/10 (2008).

69. *Id.*

70. *Id.*

71. *See id*. § 14/15.

72. *Id.* § 14/15(a).

(3) receives a written release executed by the subject of the biometric identifier or biometric information or the subject's legally authorized representative.[73]

This notice provision resulted in multiple class action lawsuits, which eventually were consolidated into one case against the social media behemoth Facebook.[74] The plaintiffs in *In re Facebook Biometric Information Privacy Litigation* alleged that Facebook's "Tag Suggestions" technology—a tool that helped identify people in photos uploaded to Facebook—violated BIPA's notice and consent requirements.[75] Similar technology was the subject of a lawsuit against Google, when the plaintiff also asserted a BIPA violation for Google's failure to notify users and obtain consent before capturing their face geometry in images uploaded to "Google Photos," the tech giant's cloud-based photo platform.[76]

Companies found to be in violation of BIPA, regardless of whether the violation was intentional or not, may be liable for damages and attorneys' fees and costs, including expert witness fees and other litigation expenses.[77] If the violation was negligent, BIPA entitles the prevailing party to seek liquidated damages of $1,000 or actual damages, whichever is greater, for each violation.[78] If the violation was intentional or reckless, each violation may cost the offending company the greater of liquidated damages of $5,000 or actual damages for each violation.[79] Additionally, equitable relief, including an injunction, may be available to a plaintiff "as the State or federal court may deem appropriate."[80]

Only under Illinois law can consumers hold companies responsible for violating their biometric information privacy. No other state or federal law

---

73. *Id.* § 14/15.

74. *In re* Facebook Biometric Info. Privacy Litig., 185 F. Supp. 3d 1155, 1159 (N.D. Cal. 2016).

75. *Id.*

76. Rivera v. Google, Inc., 238 F. Supp. 3d 1088, 1090 (N.D. Ill. 2017).

77. COMP. STAT. § 14/20.

78. *Id.* § 14/20(1).

79. *Id.* § 14/20(2).

80. *Id.* § 14/20(4).

provides consumers with such a right, at least not yet. While BIPA has flaws, the strength of the statute provides the strongest rights for consumers concerned about protecting their biometric information.[81]

III. A LANDMARK CASE FOR MODERN PRIVACY RIGHTS

In *Rosenbach v. Six Flags*, the Illinois Supreme Court settled a split among Illinois courts when it held that a violation of BIPA deprives a person of their privacy rights.[82] The violation is "no mere technicality. The injury is real and significant."[83] Unlike a password, bank account number, or social security number, if a person's biometric information is compromised, there is no easy way to fix the situation.[84] A consumer cannot request a new voice or fingerprint. Understanding the heightened sensitivity of biometric information, the court in *Rosenbach* concluded that when a company violates the statute, that violation constitutes harm sufficient for an individual to bring a cause of action against the company.[85]

The case stems from fourteen-year-old Alexander Rosenbach's school field trip to Six Flags Great America in Gurnee, Illinois.[86] Before he ventured to the amusement park, his mother, Stacy Rosenbach, purchased a season pass for Alexander online.[87] He would then complete the sign-up process for his season pass at Six Flags.[88] On the day of Alexander's field trip, he scanned his thumb at a security checkpoint at the park, and then he obtained his season pass card at a nearby administrative building.[89] On future

---

81. *See* Carra Pope, *Biometric Data Collection in an Unprotected World: Exploring the Need for Federal Legislation Protecting Biometric Data*, 26 J.L. & POL'Y 769, 791 (2018).

82. *See* Rosenbach v. Six Flags Entm't Corp., 129 N.E.3d 1197, 1204 (Ill. 2019) (*compare* Rosenbach v. Six Flags Entm't Corp., 2017 IL App (2d) 170317, *with* Sekura v. Krishna Schaumburg Tan, Inc., 115 N.E.3d 1080, 1096–99 (Ill. 2018)).

83. *Rosenbach*, 129 N.E.3d at 1206.

84. COMP. STAT. § 14/5(c).

85. *Rosenbach*, 129 N.E.3d at 1206–07.

86. *Id.* at 1200.

87. *Id.*

88. *Id.*

89. *Id.*

visits to Six Flags, the combination of Alexander's thumbprint and season pass card would allow him to enter the park quickly.[90]

When Alexander returned home from the field trip, his mother learned about the fingerprinting process for season pass holders for the first time.[91] Alexander, however, could not provide his mother with any additional information.[92] He did not receive any paperwork from Six Flags regarding his season pass or the fingerprint entry system.[93] Neither Alexander nor his mother received written notice or provided written consent for the capture or use of Alexander's thumbprint.[94] Likewise, they did not know how Alexander's biometric data would be stored or for how long.[95] Six Flag's policy regarding biometric information of season pass holders was unknown.[96]

This uncertainty led Stacy Rosenbach to file a lawsuit on her son's behalf against Six Flags.[97] In the lawsuit, Rosenbach alleged that Six Flags violated her son's privacy and failed to adhere to BIPA.[98] Rosenbach sought damages, requested injunctive relief, and asserted a common-law action for unjust enrichment.[99]

Six Flags then filed a motion to dismiss asserting that Alexander "had suffered no actual or threatened injury and therefore lacked standing to sue."[100] Additionally, Six Flags argued that the complaint failed to state a

---

90. *Id.*

91. *Id.* at 1200–01.

92. *Id.* at 1200.

93. *Id.*

94. *Id.* at 1201.

95. *Id.*

96. *Id.*

97. *See id.* at n.1 (citing Blue v. People, 585 N.E.2d 625 626, (Ill. 1992) ("A next friend of a minor is not a party to the litigation but simply represents the real party, who, as a minor, lacks capacity to sue in his or her own name.")).

98. *Rosenbach*, 129 N.E.3d at 1201.

99. *Id.*

100. *Id.* at 1201–02.

cause of action for a BIPA violation and for unjust enrichment.[101] In response, the circuit court dismissed only the unjust enrichment claim.[102] Six Flags then sought interlocutory review to resolve two questions of law.[103] Upon granting review, the intermediate appellate court analyzed: (1) the meaning of an "aggrieved person," and (2) available remedies for a person who has been aggrieved by a company in violation of BIPA.[104] The appellate court held that "a plaintiff is not 'aggrieved' within the meaning of the Act and may not pursue either damages or injunctive relief under the Act based solely on a defendant's violation of the statute. Additional injury or adverse effect must be alleged."[105] The appellate court emphasized that a technical violation of BIPA was insufficient to bring a claim under the statute.[106]

On January 25, 2019, the Illinois Supreme Court reversed the intermediate appellate court's decision.[107] The court held that a violation of BIPA is sufficient harm for a consumer to bring a cause of action.[108] "[W]hen a private entity fails to comply with one of [BIPA]'s requirements, that violation constitutes an invasion, impairment, or denial of the statutory rights of any person or customer whose biometric identifier or biometric information is subject to the breach."[109]

IV. ANALYSIS OF THE ILLINOIS SUPREME COURT'S DECISION

With careful analysis of statutory language, legislative intent, precedent, and an understanding of the unique nature of biometric information, the Illinois Supreme Court correctly held that actual injury resulting from a

101. *Id.*

102. *Id.* at 1202.

103. *Id.*

104. *Id.*

105. *Id.*

106. *Id.* (summarizing the appellate court's finding that "injury or adverse effect need not be pecuniary," but it must be more than a statutory violation).

107. *Id.* at 1200.

108. *Id.* at 1206.

109. *Id.*

BIPA violation is not required to bring a cause of action under the statute.[110] In fact, actual injury would likely mean that a person's biometric data has been compromised, in which case BIPA would have failed to accomplish precisely what the legislature intended the statute to do.

A. The Court Got It Right

In *Rosenbach v. Six Flags*, the Illinois Supreme Court analyzed the meaning of an "aggrieved person" under the state's Biometric Information Privacy Act.[111] The statute provides a private right of action for any person "aggrieved" by a BIPA violation.[112] The definition of "aggrieved," however, is not included in the statute.[113] Accordingly, the court in *Rosenbach*, like several appellate and trial courts before it, faced the question of whether "some actual injury or adverse effect," in addition to a BIPA violation, is required for a consumer to bring a cause of action.[114]

1. The Illinois Legislature Enacted BIPA to Protect, Not Limit, Privacy Rights

BIPA begins with a section on legislative findings and intent.[115] In seven clauses, the legislature provides an overview of what biometrics are, how businesses use them, and why the public is wary of utilizing biometric information in everyday life.[116] In the last clause of the preamble, the legislature concludes its intentions by stating, "[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."[117]

---

110. *Id.* at 1206.

111. *Id.* at 1199–1200.

112. *Id.*; Biometric Information Privacy Act, 740 ILL. COMP. STAT. § 14/20 (2008).

113. COMP. STAT. § 14/20.

114. *Rosenbach*, 129 N.E.3d at 1200.

115. *See* COMP. STAT. § 14/5.

116. *Id.* § 14/5(a)–(g).

117. *Id.* § 14/5.

This section of the act suggests that lawmakers in Illinois were both aware and concerned about the risks of using biometric information.[118] Prior to enacting BIPA, lawmakers in Illinois witnessed a now notorious company, Pay By Touch, crumble in controversy, litigation and eventually bankruptcy.[119] The company provided millions of consumers in Illinois with a system that allowed them to make everyday purchases with their fingerprints, instead of writing a check or swiping a credit card.[120] However, when Pay By Touch filed for bankruptcy, no one knew what would happen to all of the biometric data that it had collected.[121]

In enacting BIPA, the legislature considered how consumers might use, or not use, businesses and services in the state given the uncertainty surrounding biometric information.[122] In fact, the legislature acknowledged that "[t]he full ramifications of biometric technology are not fully known" and "many members of the public are deterred from partaking in biometric identifier-facilitated transactions."[123]

In *Rosenbach*, the Illinois Supreme Court acknowledged the legislature's intent, asserting that "[w]hen construing a statute, [the court's] primary objective is to ascertain and give effect to the legislature's intent."[124] To determine the legislature's intent, the court analyzed the language of BIPA, relying on the principle: "When the statutory language is plain and unambiguous, we may not depart from the law's terms by reading into it

118. Rivera, *supra* note 55, at 594.

119. Justin O. Kay, *The Illinois Biometric Information Privacy Act*, ASS'N OF CORP. COUNS., https://www.acc.com/sites/default/files/2019-02/Drinker-Biddle-2017-1-BIPA-Article-2.pdf [https://perma.cc/XBN3-9GCQ]; Eric Siu, *Surprising Lessons From Companies That Failed Despite A Fail-Proof Product*, FORBES (Sept. 18, 2014, 9:00 AM), https://www.forbes.com/sites/theyec/2014/09/18/surprising-lessons-from-companies-that-failed-despite-a-fail-proof-product/#52c0904d6887 [https://perma.cc/LGD3-4HQD].

120. Kay, *supra* note 120.

121. *Id.*

122. *See* COMP. STAT. § 14/5(c)–(e).

123. *Id.* § 14/5(f); *id.* § 14/5(e).

124. Rosenbach v. Six Flags Entm't Corp., 129 N.E.3d 1197, 1204 (Ill. 2019).

exceptions, limitations, or conditions the legislature did not express, nor may we add provisions not found in the law."[125]

Defendant Six Flags argued that the statute provides a private right of action only for plaintiffs who sustain actual injury.[126] In the eyes of Six Flags, violating BIPA is insufficient grounds for Rosenbach, or any other plaintiff, to bring legal action under the statute.[127] In other words, a plaintiff cannot sue based solely on a statutory violation and nothing else. The court disagreed and found the defendant's interpretation of the statute "untenable."[128]

The court likened BIPA to the state's AIDS Confidentiality Act, which does not require actual damages for recovery.[129] Under that statute, a plaintiff need not prove actual damages to bring a cause of action.[130] The statute, like BIPA, provides a private right of action to anyone "aggrieved" by a statutory violation.[131] This is in contrast to the state's Consumer Fraud and Deceptive Business Practices Act, which requires a plaintiff to allege actual damages. Under Section 10a(a) of that act, "[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."[132]

The court acknowledged that comparing the language of two separate statutes is only instructive.[133] One word could have multiple meanings depending on the context.[134] "Accepted principles of statutory construction, however, compel the conclusion that a person need not have sustained actual

---

125. *Id*. (citing Acme Markets. Inc. v. Callanan, 923 N.E.2d 718, 724 (Ill. 2009)).

126. *Id.*

127. *Id.*

128. *Id.*

129. *Id.*; *see* AIDS Confidentiality Act, 410 ILL. COMP. STAT. § 305/13 (West 2016).

130. *Id.* (citing Doe v. Chand, 781 N.E.2d 340, 351 (Ill. 2002)).

131. *Id.* (citing AIDS Confidentiality Act, 410 ILL. COMP. STAT. § 305/13 (West 2016)).

132. Consumer Fraud and Deceptive Business Practices Act, 815 ILL. COMP. STAT. § 505/10a(a) (West 2019).

133. *Rosenbach*, 129 N.E.3d at 1205.

134. *Id.* (citing People v. Ligon, 48 N.E.3d 654, 665 (Ill. 2016)).

damage beyond violation of his or her rights under the Act in order to bring an action under it."[135]

If the legislature had intended to limit the private right of action, as Six Flags argued, Illinois lawmakers would have drafted the statute to clearly communicate that.[136] Instead, the legislature enacted BIPA with the intent to provide the people of Illinois with safety and security by regulating the collection and use of biometric data.[137] A violation of the statute, however, deprives consumers of that safety and security.[138]

2. Violating a Person's Right to Privacy Is Harmful

BIPA provides an opportunity for recovery to any person "aggrieved" by a statutory violation.[139] Although the statute does not define the term "aggrieved," the court in *Rosenbach* "assume[d] the legislature intended for it to have its popularly understood meaning."[140] The court first referenced a case from 1913 where the Illinois Supreme Court found "aggrieved" to mean "'having a substantial grievance; a denial of some personal or property right.'"[141] Citing numerous other cases, the court found that Illinois courts have consistently applied this meaning of the term "aggrieved" throughout the last century.[142]

---

135. *Id.*

136. *Id.* at 1204.

137. *See* Biometric Information Privacy Act, 740 ILL. COMP. STAT. § 14/5(g) (2008).

138. *Id.*

139. *Id.* § 14/20.

140. *Rosenbach*, 129 N.E.3d at 1205.

141. *Id*. (citing Glos v. People, 102 N.E. 763, 766 (Ill. 1913)).

142. *Id*. (citing Am. Surety Co. v. Jones, 51 N.E.2d 122 (Ill. 1943); *In re* Hinshaw's Estate, 153 N.E.2d 422 (Ill. 1958); *In re* Estate of Harmston, 295 N.E.2d 66 (Ill. 1973); Greeling v. Abendroth, 813 N.E.2d 768 (Ill. 2004)).

Next, the court turned to the dictionary. In Merriam-Webster's Collegiate Dictionary, "aggrieved" means "suffering from an infringement or denial of legal rights."[143] Black's Law Dictionary defines "aggrieved" as "having legal rights that are adversely affected."[144]

Focusing on those definitions and the legislature's use of the word "aggrieved" within the context of the statute, the court concluded that a person is "aggrieved" when a company violates that person's statutory rights under BIPA.[145] In other words, a violation of BIPA is a violation of a consumer's right to privacy and control over biometric information.[146] BIPA codified those rights for consumers.[147]

Under BIPA, consumers must receive written notice, including details about the purpose and timing of the collection, storage, and use of biometric data, *before* a private entity collects or stores any biometric information.[148] In addition to obtaining written consent from a consumer, private entities are forbidden from sharing, selling, or disclosing biometric data, unless one of four exceptions is satisfied.[149] These explicit rights are precisely what the court in *Rosenbach* aimed to protect. By applying the plain meaning of "aggrieved," the court held that a company's failure to comply with BIPA results in "an invasion, impairment, or denial of the statutory rights of any person

143. *Rosenbach*, 129 N.E.3d at 1205.

144. *Id.*

145. *Id.* at 1206.

146. *Id.*

147. *Id.*

148. Biometric Information Privacy Act, 740 ILL. COMP. STAT. § 14/15(c) (2008).

149. *See id.* § 14/15(d) ("No private entity in possession of a biometric identifier or biometric information may disclose, redisclose, or otherwise disseminate a person's or a customer's biometric identifier or biometric information unless: (1) the subject of the biometric identifier or biometric information or the subject's legally authorized representative consents to the disclosure or redisclosure; (2) the disclosure or redisclosure completes a financial transaction requested or authorized by the subject of the biometric identifier or the biometric information or the subject's legally authorized representative; (3) the disclosure or redisclosure is required by State or federal law or municipal ordinance; or (4) the disclosure is required pursuant to a valid warrant or subpoena issued by a court of competent jurisdiction.").

or customer whose biometric identifier or biometric information is subject to the breach."[150]

According to the court in *Rosenbach*, requiring that someone sustain an actual injury or be a victim of a data breach is "completely antithetical to the Act's preventative and deterrent purposes."[151] In its analysis, the court referenced *Patel v. Facebook*, one of three BIPA class action cases, that was heard in the Northern District of California about a year before it was consolidated into *In re Facebook Biometric Information Privacy Litigation*.[152] The plaintiffs in *Patel* used Facebook's social networking site and alleged BIPA violations resulting from Facebook's "Tag Suggestions" feature for photos uploaded to the platform.[153] The tool used facial recognition technology to provide users with suggestions of other people to "tag" in the photo.[154] The plaintiffs alleged that Facebook violated BIPA by collecting and using their biometric information without their consent.[155]

Facebook, like Six Flags in *Rosenbach*, argued that collecting biometric information without providing notice or obtaining consent was insufficient grounds for bringing a cause of action.[156] According to Facebook, a plaintiff must experience "*real-world* harms" to bring a claim.[157] The Northern District of California disagreed.[158] Pointing to the language and provisions of the statute, the court found BIPA to be clear: "When an online service simply disregards the Illinois procedures, as Facebook is alleged to have done, the right of the individual to maintain her biometric privacy vanishes

150. *Rosenbach*, 129 N.E.3d at 1206.

151. *Id.* at 1207.

152. *Id*. at 1206; *see* Patel v. Facebook, Inc., 290 F. Supp. 3d 948 (N.D. Cal. 2018).

153. *Patel*, 290 F. Supp. 3d at 951.

154. *Id.*

155. *Id.*

156. *Id.* at 954.

157. *Id.*

158. *Id.*

into thin air. The precise harm the Illinois legislature sought to prevent is then realized."[159]

BIPA is a statute that aims to prevent harm.[160] "[P]ublic welfare, security, and safety" depend on it.[161] In the statute, the legislature emphasized the importance of protecting biometric information because "once compromised, the individual has no recourse, is at heightened risk for identity theft, and is likely to withdraw from biometric-facilitated transactions."[162]

3. Transparency and Control Are Essential to Biometric Privacy

In *Rosenbach*, the Illinois Supreme Court affirmed that BIPA "vests in individuals and customers the right to control their biometric information."[163] Before consumers can control their data, they must know what is happening with their data. Accordingly, section 15 of BIPA requires a private entity to follow specific standards for notifying consumers and obtaining written consent before capturing biometric information.[164] For example, written notification must include details about what biometric information will be collected, why it is being collected, and for how long the information will be used and stored.[165]

Notice is a fundamental principle of consumer protection law. That principle is even more important as interactions and transactions increasingly occur online, where information flows freely. In a Federal Trade Commission (FTC) report, the FTC urged companies to "increase the transparency of their data practices."[166] The FTC proposed a number of measures to achieve transparency, including presenting consumers with choices regard-

159. *Id.*

160. Rosenbach v. Six Flags Entm't Corp., 129 N.E.3d 1197, 1206 (Ill. 2019).

161. Biometric Information Privacy Act, 740 ILL. COMP. STAT. § 14/15(c) (2008).

162. *Rosenbach*, 129 N.E.3d at 1206 (citing COMP. STAT. § 14/15(c)).

163. *Rosenbach*, 129 N.E.3d at 1206.

164. COMP. STAT. § 14/15.

165. *Id.*

166. *Protecting Consumer Privacy in an Era of Rapid Change: Recommendations for Businesses and Policymakers*, FED. TRADE COMMISSION, at 1, 60 (Mar. 2012).

ing their data, making privacy statements clear and short, providing consumers with access to their data, and educating consumers about how companies collect, use, and store their data.[167]

The International Biometrics + Identity Association (IBIA), an international trade group that advocates for the responsible use of technology, echoes this philosophy.[168] To address industry-wide issues related to safety, privacy, and uniform standards, the IBIA's privacy principles articulate the need for safeguards to prevent the misuse of biometric information.[169] Within the private sector, policies must "clearly set forth how identification data will be collected, stored, accessed, and used, and . . . preserve the rights of individuals to limit the distribution of the data beyond the stated purposes."[170]

Updating privacy practices cannot come fast enough for consumers, many of whom believe they lack control of their data.[171] According to a Pew Research poll, only 9% of those surveyed believe they have "a lot of control" over information that is collected about them.[172] At the same time, 61% of people said they would like to do more to protect their privacy.[173]

Although Illinois passed BIPA more than a decade ago, the preamble suggests that the legislature anticipated the increased use of biometrics.[174] Before BIPA, Illinois was already seeing "new applications of biometric-

---

167. *Id.*

168. *Who We Are*, INT'L BIOMETRICS + IDENTITY ASS'N, https://www.ibia.org/who-we-are-ibia [https://perma.cc/9K5K-WTYL].

169. *Privacy Principles*, INT'L BIOMETRICS + IDENTITY ASS'N, https://www.ibia.org/privacy-principles [https://perma.cc/T4PH-DMCM].

170. *Id.*

171. Mary Louise Kelly, *Most Americans Feel They've Lost Control of Their Online Data*, NPR (Apr. 10, 2018, 7:02 PM), https://www.npr.org/2018/04/10/601148172/most-americans-feel-theyve-lost-control-control-of-their-online-data [https://perma.cc/9864-TQSJ].

172. Lee Rainie, *Americans' Complicated Feelings About Social Media in an Era of Privacy Concerns*, PEW RES. CTR. (Mar. 27, 2018), https://www.pewresearch.org/fact-tank/2018/03/27/americans-complicated-feelings-about-social-media-in-an-era-of-privacy-concerns/ [https://perma.cc/DH8P-LLJM].

173. *Id.*

174. Biometric Information Privacy Act, 740 ILL. COMP. STAT. § 14/5(a)–(g) (2008).

facilitated financial transactions, including finger-scan technologies at grocery stores, gas stations, and school cafeterias."[175] Since then, consumers have grown more comfortable with the use of biometrics.[176] In a study conducted by IBM Security, 67% of nearly 4,000 adults surveyed around the globe said they were comfortable using biometric authentication.[177] Among young respondents aged twenty-to-thirty-six-years old, 75% said they comfortably use biometrics.[178] Nevertheless, security of information remains a priority. In the IBM survey, respondents prioritized security over convenience and privacy.[179] That was especially true when logging in to financial applications.[180]

Security is clearly defined as a priority under BIPA.[181] To keep information secure and thus prevent harm, BIPA provides safeguards "to insure that individuals' and customers' privacy rights in their biometric identifiers and biometric information are properly honored and protected . . . *before* they are or can be compromised."[182]

4. A Law That Holds Companies Accountable Encourages Compliance

BIPA incentivizes businesses that collect or use biometric information in Illinois to comply with the statute.[183] Businesses that fail to adhere to the

175. *Id.* § 14/5(b).

176. Limor Kessem, *IBM Study: Consumers Weigh in on Biometrics, Authentication and the Future of Identity*, SECURITY INTELLIGENCE (Jan. 29, 2018), https://securityintelligence.com/new-ibm-study-consumers-weigh-in-on-biometrics-authentication-and-the-future-of-identity/ [https://perma.cc/252V-XCNG].

177. *Id.*

178. *Id.*

179. *Id.*

180. *Id.*

181. *See* Biometric Information Privacy Act, 740 ILL. COMP. STAT. § 14/5(g) (2008).

182. Rosenbach v. Six Flags Entm't Corp., 129 N.E.3d 1197, 1206–07 (Ill. 2019) (emphasis added).

183. *Id.* at 1207.

requirements of BIPA risk liability, "including liquidated damages, injunctions, attorneys' fees, and litigation expenses 'for each violation' of the law whether or not actual damages, beyond violation of the law's provisions, can be shown."[184] The risk for companies is even higher with the private right of action. Under *Rosenbach*, a violation of BIPA with no additional injury, provides consumers with grounds to bring legal action.[185] That risk should compel companies to comply with the statute and "prevent problems before they occur and cannot be undone."[186]

Rosenbach serves as a warning to businesses that operate in Illinois and collect or use biometric information.[187] Following the decision, news reports, law firm blogs, and privacy advocates chronicled the landmark case, coupling it with a call-to-action for businesses in Illinois to evaluate their business policies and practices.[188] "The tech industry insists that consumers shouldn't be able to take companies to court merely because the companies violate privacy laws," said Neema Singh Guliani, senior legislative counsel at the American Civil Liberties Union.[189] "We applaud the Illinois Supreme

184. *Id.*

185. *Id.*

186. *Id.*

187. Wessler, *supra* note 29.

188. *See* Ally Marotti, *Illinois Supreme Court Rules Against Six Flags in Lawsuit over Fingerprint Scans. Here's Why Facebook and Google Care*, CHI. TRIB. (Jan. 25, 2019, 10:30 AM), https://www.chicagotribune.com/business/ct-biz-six-flags-biometrics-lawsuit-20190125-story.html [https://perma.cc/VJY5-MZW3]; Carlton Fields & Joseph Swanson, *No Actual Harm Needed to Sue Under BIPA: Illinois Supreme Court Finds Statutory Violation Sufficient*, JD SUPRA (Jan. 31, 2019), https://www.jdsupra.com/legalnews/no-actual-harm-needed-to-sue-under-bipa-97869/. [https://perma.cc/U59Y-EJDS]; Wessler, *supra* note 29; Malhortra et al., *supra* note 29; Jeffrey Widman, *Illinois Supreme Court Rules That Actual Damages Are Not Necessary Under the Illinois Biometric Information Privacy Act*, FOX ROTHSCHILD LLP ATTORNEYS AT LAW (Feb. 6, 2019), https://dataprivacy.foxrothschild.com/2019/02/articles/right-to-privacy/illinois-supreme-court-rules-that-actual-damages-are-not-necessary-under-the-illinois-biometric-information-privacy-act/ [https://perma.cc/TWF6-3V6L].

189. Katharine Schwab, *A Landmark Ruling Gives New Power to Sue Tech Giants for Privacy Harms*, FAST COMPANY (Jan. 26, 2019), https://www.fastcompany.com/90297382/illinois-supreme-court-decision-marks-a-landmark-win-for-biometric-privacy-harm [https://perma.cc/UGG6-YANU].

Court for rejecting these self-serving arguments and making clear that companies that fail to comply with Illinois' biometric law can be sued for damages."[190]

The possibility of a class action lawsuit, if nothing else, should motivate companies operating in Illinois to evaluate their use of biometric technology.[191] Simply from a financial perspective, companies should consider the potential economic impact of operating biometric technology in Illinois.[192] At a minimum, taking steps to strengthen privacy practices, such as disclosures and consent, would help mitigate the risk of litigation and the potential liability for damages.[193]

According to *Rosenbach*, compliance with BIPA should be manageable.[194] The court found that "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[.]"[195] In fact, the Illinois legislature alluded to this in the preamble of the statute.[196] "The full ramifications of biometric technology are not fully known."[197] As more companies collect, use, and store biometric information, databases containing biometric identifiers grow, and the risk of a devastating data breach increases.[198] If stolen, a consumer's biometric information could be used to access sensitive personal information, thereby increasing the risk of tangible harm to the consumer.[199]

---

190. *Id.*

191. Deal et al., *supra* note 67, at 19.

192. *Id*.

193. *Id.*; *see also* Fields & Swanson, *supra* note 189.

194. *See* Rosenbach v. Six Flags Entm't Corp., 129 N.E.3d 1197, 1207 (Ill. 2019).

195. *Id.*

196. *See* Biometric Information Privacy Act, 740 ILL. COMP. STAT. § 14/5(f) (2008).

197. *Id.*

198. Elias Wright, *The Future of Facial Recognition Is Not Fully Known: Developing Privacy and Security Regulatory Mechanisms for Facial Recognition in the Retail Sector*, 29 FORDHAM INTELL. PROP. MEDIA & ENT. L.J. 611, 629 (2019).

199. *Id.*

To provide protection for consumers and to ensure compliance with the provisions of BIPA, companies can plan ahead by incorporating a consumer's privacy rights into the development of new technologies.[200] This means bringing lawyers into projects early, instead of having an attorney review a nearly completed product or technology that will soon be consumer-facing.[201] Contemplating the law, in addition to general privacy and cybersecurity concerns, during the innovation process would allow companies to more easily comply with privacy statutes, such as BIPA, down the road.[202] This is particularly important as technology advances and the collection of biometric information becomes ubiquitous.[203] Without proper notice and consent requirements, privacy groups warn that consumers will not know if, when, where, and why companies collect personal information, such as biometric identifiers.[204]

For example, the improvement of facial recognition technology allows devices to scan the faces and eyes of people from greater distances.[205] In a survey conducted by the American Civil Liberties Union, eighteen of the top twenty retail companies in the United States refused to reveal whether they employed technology that scanned the faces of customers.[206] Unless the law requires companies to notify customers and obtain informed consent before

200. *See* Michael Bahar et al., *Lawyers at the Vanguard: The Wisdom of Involving Lawyers at the Innovative Design Phases, and the Obligations on Those Lawyers*, FINTECH L. REP., Mar.-Apr. 2019, at 1, 5.

201. *See id.*

202. *See id.*

203. Brief of Amici Curiae The Am. Civil Liberties Union et al. in Support of Plaintiff-Appellant at 8, Rosenbach v. Six Flags Entertainment Corp., 129 N.E.3d 1197 (Ill. 2019) (No. 123186).

204. *Id.*

205. *Id.* at 7.

206. *Id.* (citing Jenna Bitar & Jay Stanley, *Are Stores You Shop at Secretly Using Face Recognition on You?*, AM. CIV. LIBERTIES UNION (Mar. 26, 2018, 4:15 PM), https://www.aclu.org/blog/privacy-technology/surveillance-technologies/are-stores-you-shop-secretly-using-face) [https://perma.cc/KQM2-Z4NJ]).

a company utilizes facial recognition technology, companies may never inform consumers about the collection of their biometric information.[207]

Beyond notice and consent, BIPA requires businesses in possession of biometrics to "store, transmit, and protect from disclosure all biometric identifiers and biometric information in a manner that is the same as or more protective than the manner in which the private entity stores, transmits, and protects other confidential and sensitive information."[208] This provision imposes a "reasonable standard of care" on businesses,[209] requiring them to think not only about the collection of biometrics, but also about how the data will be stored and managed. With the rise of hacks and data breaches, companies must protect sensitive information.[210]

B. A Lower Standard for Harm

The impact of *Rosenbach* is significant for both consumers and companies in Illinois. Following the case, if a company fails to notify a consumer about their collection of biometric identifiers, or if a company improperly manages biometric information, a consumer may bring legal action against that company.[211] Illinois consumers can sue companies for violating BIPA without proving actual damages.[212] As the court explained, "[n]o additional consequences need be pleaded or proved."[213] The statutory violation alone is sufficient grounds for a private right of action.[214]

---

207. Brief of Amici Curiae The Am. Civil Liberties Union et al. in Support of Plaintiff-Appellant at 9, Rosenbach v. Six Flags Entertainment Corp., 129 N.E.3d 1197 (Ill. 2019) (No. 123186).

208. Biometric Information Privacy Act, 740 ILL. COMP. STAT. § 14/15(e)(2) (2008).

209. *Id.* § 14/15(e)(1).

210. *See* Wright, *supra* note 199, at 629.

211. *Rosenbach*, 129 N.E.3d at 1206; *see* COMP. STAT. § 14/20.

212. *Rosenbach*, 129 N.E.3d at 1200.

213. *Id.*

214. *Id.*

This reasoning differs from the conclusions of some earlier BIPA cases litigated in state and federal district courts in Illinois.[215] Additionally, the holding in *Rosenbach* conflicts with the United States Supreme Court's interpretation of constitutional standing, as articulated in *Spokeo, Inc. v. Robins*, a notable case that addressed whether a statutory violation constituted an injury sufficient for standing in federal court.[216] Effectively, *Rosenbach* deviated from traditional interpretations of standing and lowered the threshold for a consumer's right to sue for a statutory violation—a threshold that traditionally requires the pleading of actual harm.

1. Generally, Consumers Must Demonstrate Actual Harm

Prior to the Illinois Supreme Court's decision in *Rosenbach*, courts were split on the standing requirement under BIPA.[217] The statute provides a private right of action for an "aggrieved" person, but the statute does not define "aggrieved."[218] Subsequently, courts analyzed the meaning of "aggrieved" and whether a plaintiff could bring a cause of action under BIPA without alleging actual harm. The issue turned on standing and what a plaintiff must plead in order to bring a case under BIPA.

In 2016, the United States Supreme Court answered a similar standing question in *Spokeo*, affirming its prior position that a plaintiff must allege an injury that is "both 'concrete *and* particularized'" to meet the injury-in-fact requirement of Article III standing in federal court.[219] A "concrete" injury must be real, actual or imminent.[220] For the injury to be "particularized," the plaintiff must have personally suffered.[221] Applying those principles to the plaintiff's allegations, the Court held that a "bare procedural violation" of

---

215. *See, e.g.*, McCollough v. Smarte Carte, Inc., No. 16 C 03777, 2016 WL 4077108, at *1 (N.D. Ill. Aug. 1, 2016); Rivera v. Google, Inc., 366 F. Supp. 3d 998, 1001 (N.D. Ill. 2018); *see also* Deal et al., *supra* note 67, at 18–19.

216. *See* Spokeo, Inc. v. Robins, 136 S. Ct. 1540 (2016).

217. *See Rosenbach*, 129 N.E.3d at 1204.

218. *See* Biometric Information Privacy Act, 740 ILL. COMP. STAT. § 14/20 (2008).

219. *Spokeo*, 136 S. Ct. 1540 at 1545 (italics added) (quoting Friends of the Earth, Inc. v. Laidlaw Envtl. Servs. (TOC), Inc., 528 U.S. 167, 180–81 (2000)).

220. *Id.* at 1548.

221. *Id.*

the Fair Credit Reporting Act (FCRA) failed to meet the constitutional requirement for standing.[222] The Court focused on what constitutes actual harm, finding that:

> A violation of one of the FCRA's procedural requirements may result in no harm. For example, even if a consumer reporting agency fails to provide the required notice to a user of the agency's consumer information, that information regardless may be entirely accurate. In addition, not all inaccuracies cause harm or present any material risk of harm.[223]

Without allegations of concrete harm, the Court held that a statutory violation alone failed to meet the injury-in-fact requirement of Article III standing.[224]

Relying on *Spokeo*, the district court in *McCollough v. Smarte Carte, Inc.* applied the principles of constitutional standing to a BIPA case in the Northern District of Illinois.[225] There, a consumer who used her fingerprint to open a storage locker at a train station claimed that she did not receive notice or provide consent to the collection and use of her fingerprint.[226] The court acknowledged that the facts showed a "technical violation" of BIPA, but because the plaintiff failed to allege "any harm that resulted from the violation," the plaintiff lacked constitutional standing.[227] Furthermore, the district court held that the plaintiff also lacked statutory standing under BIPA for alleging facts to show that the defendant company's violation of the statute adversely affected her privacy rights.[228] As a result, the court found that

---

222. *Id.* at 1550.

223. *Id.*

224. *Id.* at 1549.

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

226. *Id.*

227. *Id.* at *3.

228. *Id.* at *4.

the plaintiff did not fit the definition of an "aggrieved" party who could bring a lawsuit against a company under BIPA.[229]

That interpretation surfaced again when the Second District of the Illinois Appellate Court analyzed the *Rosenbach* case.[230] The intermediate appellate court held that a plaintiff must allege more than a technical violation of the statute to bring a cause of action.[231] Under the statute, the appellate court interpreted an "aggrieved" person as someone who sustained an actual injury or experienced an adverse effect.[232] A violation of BIPA, and nothing more, was simply insufficient for bringing a cause of action under the statute.[233] The appellate court concluded that the legislature would have omitted the word "aggrieved" if it intended to provide a right of action to consumers every time an entity violated BIPA.[234]

2. Redefining Harm in the Digital Age

In its reversal of the intermediate appellate court's decision, the Illinois Supreme Court in *Rosenbach* rejected the idea that a statutory violation, in itself, does not constitute harm sufficient for standing.[235] The court expressed an understanding of how easily technology can invade a person's privacy, finding that a failure to comply with the provisions of BIPA is a violation of the right to privacy and the right to control deeply personal information, such as a fingerprint, voice, or face.[236] Simultaneously, the court

229. *Id.*

230. Rosenbach v. Six Flags Entm't Corp., 2017 IL App (2d), ¶¶ 20–23, 170317.

231. *Id.* ¶ 23.

232. *Id.*

233. *Id.* ¶ 28 (holding that "[i]f 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 in section 20. We note, however, that the injury or adverse effect need not be pecuniary.").

234. *Id.* ¶ 23 (finding 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.").

235. Rosenbach v. Six Flags Entm't Corp., 129 N.E.3d 1197, 1204 (Ill. 2019).

236. *See id.* at 1206.

expanded the concept of harm and injury as it exists in today's digital world.[237] Contrary to courts that previously interpreted "aggrieved" to mean a person who experienced actual harm, the court viewed the violation of a person's right to privacy as harmful.[238] In doing so, the court reminded both businesses and consumers of the broad privacy protections provided by BIPA, a statute intended to serve the public's welfare, security, and safety.[239]

Although *Rosenbach* is an outlier, the case represents a "forward-thinking judicial perspective" of standing.[240] In holding that a violation of BIPA constituted harm, the court in *Rosenbach* understood that violating a person's privacy rights is a "real and significant" injury.[241] Furthering this interpretation, the Ninth Circuit applied similar reasoning in its recent decision in *Patel v. Facebook*, a BIPA case that analyzed Article III standing in the context of allegations involving the social media giant's facial recognition technology.[242] Applying *Spokeo*, the Ninth Circuit found that a plaintiff who pleads a statutory violation, and nothing else, can satisfy the concrete injury-in-fact requirement of Article III standing, but that does not happen automatically, even if the statute itself provides a plaintiff with the right to sue.[243] The court must proceed with the standing analysis and determine whether the plaintiff suffered a concrete injury.[244] To do this, the Ninth Circuit applied a two-part test to evaluate: (1) whether the legislature enacted BIPA to protect a plaintiff's concrete interests, and (2) whether the

237. *Id.* (quoting Patel v. Facebook, Inc., 290 F. Supp. 3d 948, 954 (N.D. Cal. 2018), the court found that "[t]hese procedural protections 'are particularly crucial in our digital world because technology now permits the wholesale collection and storage of an individual's unique biometric identifiers—identifiers that cannot be changed if compromised or misused.'").

238. *Id.*; *see* Deal et al., *supra* note 67, at 18.

239. *Rosenbach*, 129 N.E.3d at 1206; Biometric Information Privacy Act, 740 ILL. COMP. STAT. § 14/5(g) (2008).

240. Rivera, *supra* note 55, at 602.

241. *Rosenbach*, 129 N.E.3d at 1206.

242. Patel v. Facebook, 932 F.3d 1264, 1270–74 (9th Cir. 2019).

243. *Id.* at 1270.

244. *Id.*

statutory violation alleged by the plaintiff caused harm or the material risk of harm.[245]

In analyzing the first part of the test, the Ninth Circuit referenced Fourth Amendment case law, specifically Supreme Court jurisprudence that evaluated advanced technology and its impact on the right to privacy.[246] With an eye toward the future, the Ninth Circuit concluded that "the development of a face template using facial-recognition technology without consent . . . invades an individual's private affairs and concrete interests."[247] The court found that the Illinois legislature enacted BIPA to protect such privacy interests, a conclusion that aligns with the Illinois Supreme Court's holding in *Rosenbach*.[248]

To address the second part of the test, the Ninth Circuit in *Patel* focused on Facebook's alleged conduct and whether their collecting, using, and storing of biometric information allegedly without written consent violated the substantive privacy rights of consumers.[249] In its articulation of the alleged facts, the Ninth Circuit suggests that the conclusion is clear: a violation of BIPA is a violation of a substantive privacy right.[250] In accordance with the Illinois Supreme Court's conclusion in *Rosenbach*, the Ninth Circuit held that "the privacy right protected by BIPA is the right not to be subject to the collection and use of such biometric data."[251] Accordingly, the Ninth Circuit held that the plaintiff Facebook users sufficiently alleged a particularized and concrete harm that satisfies Article III standing.[252]

The impact of the Ninth Circuit's decision in *Patel v. Facebook* is significant.[253] Although the case has not yet gone to trial, the holding establishes new ground for consumers, providing strong support for the protection

245. *Id.* at 1270–71.

246. *Id.* at 1272–73.

247. *Id.* at 1273.

248. *Id.*

249. *Id.* at 1274.

250. *See id.*

251. *Id.*

252. *Id.*

253. *See* Allison Grande, *Facebook Ruling Extends Life of Ill. Biometric Privacy Claims*, LAW360 (Aug. 12, 2019, 4:28 PM), https://www.law360.com/articles/1187064/facebook-ruling-

of privacy rights in the digital age.[254] Most importantly, the Ninth Circuit directly addressed the constitutional standing issue that the Illinois Supreme Court omitted in its *Rosenbach* decision.[255] Moving forward, there is now both state and federal precedent for plaintiffs satisfying standing requirements under BIPA by alleging statutory violations and no additional harm.

3. Floodgates of Litigation

Although the Illinois legislature may not have intended to encourage litigation, the Illinois Supreme Court suggested that the legislature understood the power of BIPA.[256] In *Rosenbach*, the court concluded that the legislature "intended for the provision to have substantial force."[257]

Since 2008, when the Illinois legislature enacted BIPA, there have been at least 110 lawsuits claiming statutory violations filed against businesses.[258] Plaintiffs have filed class action lawsuits against tech companies whose cutting-edge technology utilizes biometrics and employers who utilize fingerprints for secure and efficient time-keeping.[259] In numerous cases, the decision turned on whether a violation of BIPA, without alleging any other harm, provided a plaintiff with standing to sue under the statutory right of

---

extends-life-of-ill-biometric-privacy-claims (last visited Oct. 23, 2019) (reporting that *Patel v. Facebook* "is likely to widen the path for plaintiffs pursuing BIPA class actions by making it easier to get their claims into court and to certify their proposed classes. It also creates a circuit split on what type of harm is required for standing that could lead to a U.S. Supreme Court's review, attorneys say.").

254. *See id.*

255. *Compare* Patel, 932 F.3d at 1270 (analyzing the "injury in fact" requirement of Article III standing within the context of BIPA), *with* Rosenbach v. Six Flags Entm't Corp., 129 N.E.3d 1197, 1204–07 (analyzing standing under BIPA without referencing constitutional standing or *Spokeo*, a case that the *Patel* court referenced).

256. Rosenbach, 129 N.E.3d at 1207.

257. *Id.*

258. Schwab, *supra* note 190.

259. Amy Korte, *Illinois Employers Flooded With Class-Action Lawsuits Stemming from Biometric Privacy Law*, ILL. POLICY (Oct. 17, 2017), https://www.illinoispolicy.org/illinois-employers-flooded-with-class-action-lawsuits-stemming-from-biometric-privacy-law/ [https://perma.cc/8TYA-36VX].

action for "aggrieved" persons.[260] The *Rosenbach* decision answered that question in the affirmative, establishing precedent for consumers in Illinois to hold companies accountable for violating their biometric information privacy rights.[261]

While consumers and attorneys representing plaintiffs welcomed the decision, others were disappointed.[262] President and CEO of the Illinois Chamber of Commerce, Todd Maish, warned that the court's ruling in *Rosenbach* would result in more lawsuits against Illinois employers, which would ultimately injure the state's economy.[263] The decision also conflicts with the concept of "harm-focused enforcement" expressed by the U.S. Chamber of Commerce.[264] In an outline of privacy principles, the Chamber of Commerce asserted that "[e]nforcement provisions of a federal data privacy law should only apply where there is concrete harm to individuals."[265] Removing the requirement for "concrete harm," such as pecuniary damages or identity theft, allows more consumers to proactively bring lawsuits against businesses that fail to comply with the provisions of BIPA.

C. Model for Regulation

As individual states propose and enact biometric information privacy laws, liability for companies grows while the rights of consumers remain unclear. The regulations from one state to another are inconsistent, creating additional challenges for companies to comply with crucial privacy, data

---

260. *See, e.g.*, *In re* Facebook Biometric Info. Privacy Litig., 185 F. Supp. 3d 1155, 1159 (N.D. Cal. 2016); Monroy v. Shutterfly, Inc., No. 16 C 10984, 2017 WL 4099846, at *1 (N.D. Ill. Sept. 15, 2017); Rivera v. Google, Inc., 366 F. Supp. 3d 998, 1001 (N.D. Ill. 2018).

261. *Rosenbach*, 129 N.E.3d at 1206.

262. Malhortra et al., *supra* note 29.

263. Press Release, Ill. Chamber of Commerce, Illinois Chamber of Commerce Statement on Illinois Supreme Court's ruling on Rosenbach v. Six Flags (Jan. 25, 2019) (on file with author) (Todd Maish expressed fear that "today's decision will open the floodgates for future litigation at the expense of Illinois' commercial health."); *see also Court: Illinois Mom Can Sue Six Flags for Fingerprinting Son*, ASSOCIATED PRESS (Jan. 25, 2019), https://www.apnews.com/f1bc8a2d13d14be9bf83f00c5b305311 [https://perma.cc/WBG5-WRDW].

264. *See* U.S. CHAMBER OF COM., *U.S. Chamber Privacy Principles* (Sept. 6, 2018, 12:00 PM), https://www.uschamber.com/issue-brief/us-chamber-privacy-principles [https://perma.cc/7FZC-NHEF].

265. *Id.*

protection, and cybersecurity laws.[266] The current patchwork of privacy law leaves the majority of U.S. consumers without sufficient protection and security.

Rosenbach v. Six Flags exemplifies how biometric information privacy regulations should be applied. In the decision, the Illinois Supreme Court articulated key principles powering BIPA, which lawmakers should follow. Most importantly, (1) consumers have a right to control their biometric information; (2) companies must be transparent about the collection, storage, and use of consumers' biometric information; (3) companies must adhere to statutory regulations regarding biometric information privacy by complying with requirements, such as providing proper notice and consent; (4) consumers have a private right of action to hold companies accountable; and (5) if a company violates the statutory regulations, that is sufficient for a consumer to bring legal action.[267] Actual harm or damages are not required. In fact, actual harm, such as identify theft or loss of money, means it is too late—a consumer's biometric information is no longer safe. Actual harm means a consumer's privacy has been violated. These principles are the foundation for protecting consumer privacy rights nationwide.

Federal regulation would establish uniformity and enforcement on a national level. As more businesses use and collect biometric information of consumers, a standardized system of regulation becomes more necessary. Currently, the state-by-state regulation of biometric information requires businesses to be cognizant of different definitions of "biometrics" and the varying rights associated with those identifiers.[268] Without a uniform law, businesses may develop policies and procedures that are sufficient in some states and insufficient in others. This is particularly problematic given the expansive nature of operating a business that is accessible on the Internet or through a mobile app. A broadly applicable federal law would provide clarity for businesses, allowing them to innovate with privacy laws in mind.[269]

266. Pope, *supra* note 82.

267. *See generally* Rosenbach v. Six Flags Entm't Corp., 129 N.E.3d. 1197 (Ill. 2019).

268. Pope, *supra* note 82, at 799.

269. *Id.* at 797–98.

V. CONCLUSION

A landmark decision, *Rosenbach v. Six Flags* represents a modern approach to privacy rights in the United States. In the case, the Illinois Supreme Court analyzed statutory language, legislative intent, and policies regarding consumers, privacy, and technology.[270] Given the uncertainty of where technology will go and how consumers will continue to leverage their biometric information, the court correctly applied BIPA, providing plaintiffs with a right to bring a cause of action against companies, retailers, and employers that violate their rights under the statute. That private right of action is essential for accountability. Without it, privacy rights regarding biometric information remain out of reach for consumers.

Although more and more states are proposing legislation that aligns with the policies supporting BIPA, the lack of uniformity creates uncertainty for both businesses and consumers. Developing a federal law that protects biometric information privacy rights is a necessary next step. With an established standard for collecting, using, and storing biometric information, consumers would continue to benefit from innovative technology while feeling more secure about protecting their personal information.

270. *See supra* Part III; *see generally Rosenbach*, 129 N.E.3d 1197.