The Who, Why, and Where of Biometric Privacy Litigation: An Empirical Analysis of BIPA Cases 2015-2024

Blake Fensom, Jee-Yeon Lehmann, Lolo Palacios, and Shannon Seitz

I. Introduction

The use of biometric technologies[1] for identity verification has increased rapidly in the U.S. and around the world, with the global biometrics technology market estimated at $42 billion in 2023 and projected to reach $267 billion by 2033.[2] The rapid adoption of biometric technologies can be attributed in part to the enhanced security and convenience that they provide over traditional forms of authentication. Unlike passwords, PINs, or identification cards, biometric data uniquely identify an individual through that person's biological traits that are difficult to replicate, thereby reducing the risk of identity theft through stolen credentials.[3] Moreover, biometric authentication technologies are also generally more convenient and user-friendly because they eliminate the need to create and remember passwords or carry physical tokens like badges.[4]

While these advantages have been identified, the proliferation of biometric technologies is also raising new concerns about privacy and security, stemming from the fact that biometric data cannot be changed in the event that data are compromised.[5] In addition, regulators such as the Federal Trade Commission (FTC) have raised significant concerns about the potential use of biometric information for the "production of counterfeit videos or voice recordings (so-called 'deep fakes') […] to commit fraud or to defame or harass" individuals.[6]

Since there is no comprehensive federal privacy law in the U.S., an increasing number of states have enacted or are actively considering privacy laws governing the use of biometric data,[7] led

Blake Fensom *is an associate in the Toronto office of Analysis Group.* ***Jee-Yeon Lehmann*** *is a managing principal,* ***Lolo Palacios*** *is a vice president, and* ***Shannon Seitz*** *is a vice president in the Boston office of Analysis Group.* *The authors thank Josephine Kantawiria, Keegan Dolan, and Shoshana Singer for their excellent research assistance. The views expressed in this article are those of the authors only and do not necessarily represent those of Analysis Group or its clients.*

[1] We use the terms "biometric technology" and "biometric identifier" throughout this article because these terms are commonly used to describe certain technologies and identifiers in the literature. Our use of the terms "biometric technology" or "biometric identifier" does not imply that any particular technology or identifier is covered by the Illinois Biometric Information Privacy Act or other legislation governing the use of biometric information. When referring to specific cases, we accept the definition of "biometric identifiers" used in the complaints.

[2] Biometrics are measurable biological and behavioral characteristics that are unique to an individual. *See Biometrics*, U.S. DEPARTMENT OF HOMELAND SECURITY (Jan. 24, 2025), https://www.dhs.gov/biometrics; *Biometrics by the Numbers: A Deep Dive Into Trends, Adoption, and Challenges*, Oloid (Aug. 16, 2024), https://www.oloid.ai/blog/biometrics-by-the-numbers-a-deep-dive-into-trends-adoption-and-challenges/.

[3] Zhang Rui & Zheng Yan, *A Survey on Biometric Authentication: Toward Secure and Privacy-Preserving Identification*, 7 IEEE Access (2019).

[4] *Id.*

[5] Biometric Information Privacy Act, 740 ILCS 14 (2008), Section 5.

[6] *Policy Statement of the Federal Trade Commission on Biometric Information and Section 5 of the Federal Trade Commission Act*, U.S. Federal Trade Commission, https://www.ftc.gov/system/files/ftc_gov/pdf/p225402biometricpolicystatement.pdf, p. 3.

[7] Illinois, Texas, and Washington have enacted laws addressing the collection, use and protection of biometric data. In addition to these states with specific biometric privacy laws, California, Colorado, Connecticut, Utah, and Virginia have incorporated provisions related to biometric data within broader consumer privacy legislation. *See Is Biometric Information Protected by Privacy Laws?*, Bloomberg Law (June 20, 2024), https://pro.bloomberglaw.com/insights/privacy/biometric-data-privacy-laws/bipa.

Following its enactment in 2008, BIPA has served as a guide for subsequent state legislation and produced a surge of biometric privacy lawsuits across the U.S., shining a spotlight on the significant litigation and compliance risks that businesses face over the collection and use of biometric data.

by the Illinois *Biometric Information Privacy Act* (BIPA).[8] Following its enactment in 2008, BIPA has served as a guide for subsequent state legislation and produced a surge of biometric privacy lawsuits across the U.S., shining a spotlight on the significant litigation and compliance risks that businesses face over the collection and use of biometric data.

In this article, we analyze key characteristics of BIPA cases filed in U.S. federal court since 2015 and how BIPA litigation has responded to changes in the legal environment and increases in the adoption of biometric technologies. First, over the past decade, there has been a dramatic increase in the number of BIPA cases filed, particularly following the Illinois Supreme Court's ruling in *Rosenbach v. Six Flags Entertainment Corp.* in January 2019, which affected the economic incentives for plaintiffs to pursue these cases.[9] Second, we find that the biometric technologies involved in BIPA litigation largely reflect how biometric technologies have been adopted and used in the U.S. Third, the at-issue biometric identifiers—as defined by BIPA[10]—vary across plaintiff types, with allegations related to fingerprints being more common in cases filed by workers, and allegations related to face geometry being more common in cases filed by consumers. Finally, the underlying technologies at issue in BIPA cases have also continued to evolve with the introduction of new biometric technologies and changes in demand and other market factors. For example, BIPA cases involving virtual try-on tools for at-home product testing are on the rise,[11] and cases involving the use of online proctoring technologies during exams increased during COVID-19.[12]

II. Overview of BIPA

BIPA, signed into law in 2008 by then-Governor Rod Blagojevich, was the first state legislation to regulate the use of biometric information in the U.S.[13] BIPA requires private entities in possession of biometric information to (i) inform individuals about the type of biometric information being collected; (ii) describe the purpose for, and duration of, the collection, storage, and use of this information; and (iii) obtain written consent for its collection.[14] The biometric identifiers defined under BIPA include fingerprint, scan of retina or iris, scan of hand or face geometry, and voiceprint.[15]

---

[8] Biometric Information Privacy Act, 740 ILCS 14 (2008).

[9] Molly DiRago, *The Litigation Landscape of Illinois' Biometric Information Privacy Act*, American Bar Association (2021), https://www.troutman.com/a/web/288907/CyberData-Summer-2021-v2-Molly-DiRago-article.pdf, p. 38.

[10] Biometric Information Privacy Act, 740 ILCS 14 (2008), Section 10.

[11] *See, for example,* Corrected First Amended Class Action Complaint, Castelaz v. Estée Lauder Co., Inc., 2024 U.S. Dist. LEXIS 7321, 2024 WL 136872 (N.D. Ill. June 26, 2023) (No. 1:22-cv-05713-LCJ).

[12] *See, for example,* Class Action Complaint with Jury Demand, Stalcup v. Veratad Technologies, (Ill. Cir. Oct. 20, 2021) (No. 2:22-cv-0210-CSB-EIL).

[13] Bloomberg Law, *supra* note 7. *See also* Hannah Meisel, *Court Rulings Supercharge Illinois' Strongest-in-Nation Biometric Privacy Law*, Capitol News Illinois (Mar. 1, 2023), https://capitolnewsillinois.com/news/court-rulings-supercharge-illinois-strongest-in-nation-biometric-privacy-law/.

[14] *Biometric Information Privacy Act (BIPA)*, ACLU of Illinois, https://www.aclu-il.org/en/campaigns/biometric-information-privacy-act-bipa.

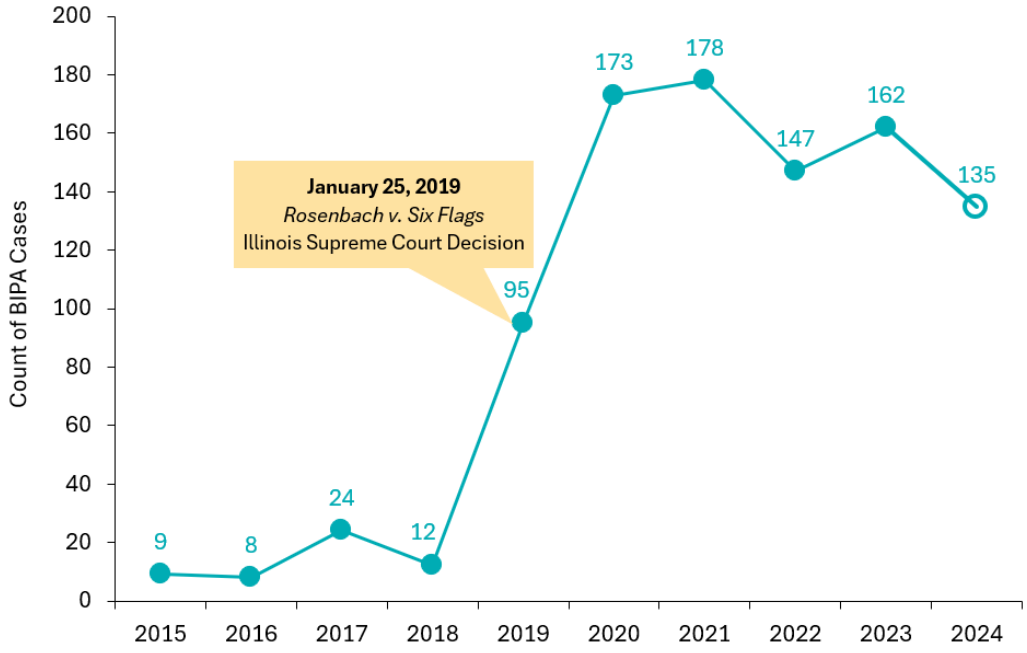
[15] Biometric Information Privacy Act, 740 ILCS 14 (2008), Section 10. BIPA also includes an extensive list of items that are not considered biometric identifiers under the law, such as writing samples, written signatures, physical descriptors such as height or eye color, and X-rays. BIPA does not apply to the collection and use of biological materials, the collection of which are regulated by the Illinois *Genetic Information Privacy Act*. *See* Genetic Information Privacy Act, 410 ILCS 513 (1998).

BIPA is also the first biometric privacy law in the U.S. with a private right of action.[16] BIPA's private right of action allows any individual "aggrieved" by a violation to seek statutory or actual damages, attorney's fees, and injunctive relief.[17] This means that an individual can hold companies accountable for issues like collecting biometric data without informed consent, failing to disclose how the data will be used or stored, or mishandling the security of the data. A prevailing party may recover "liquidated damages of $1,000 or actual damages, whichever is greater" for each negligent BIPA violation and "liquidated damages of $5,000 or actual damages, whichever is greater" for each intentional or reckless BIPA violation.[18]

Despite being enacted in 2008, BIPA litigation remained largely dormant until 2015. As shown in **Figure 1**, the number of BIPA cases remained fairly low until 2019. From 2018 to 2020, the number of BIPA cases filed in federal court increased from 12 to 173, representing more than a 13-fold increase.

Figure 1

Number of BIPA Cases by Year[19]



The large increase in the number of BIPA cases filed in federal court after 2018 is associated with a series of legal decisions that changed the incentives to litigate alleged BIPA violations.

The large increase in the number of BIPA cases filed in federal court after 2018 is associated with a series of legal decisions that changed the incentives to litigate alleged BIPA violations. The most consequential decision was the Illinois Supreme Court's ruling in *Rosenbach v. Six Flags Entertainment Corp.* in January 2019, which increased plaintiffs' incentives to file BIPA matters by lowering their burden of proof to qualify for compensation in BIPA matters. In *Rosenbach*, plaintiff Stacy Rosenbach alleged that Six Flags had improperly collected her 14-year-old son's

[16] Jalen Brown & Katherine J. Ellena, *Biometric Privacy Violations: As Costs of Liability Soar, Insurance May Respond*, Reed Smith (June 6, 2023), https://www.reedsmith.com/en/perspectives/cyber-insurance-claims/2023/06/biometric-privacy-violations-as-costs-liability-soar-insurance-may-respond.

[17] Biometric Information Privacy Act, 740 ILCS 14 (2008), Section 20.

[18] *Id.*

[19] The number of BIPA cases for the year 2024 is projected based on the cases filed in federal court during the first eight months of the year.

biometric information when he visited one of its amusement parks, where he was asked to scan his fingerprints to verify his identity for subsequent season pass access.[20] In response, Six Flags sought dismissal of the case by asserting that Stacy Rosenbach had suffered no actual harm, and, therefore, was not "aggrieved" by the alleged BIPA violations.[21] On appeal, the Illinois Supreme Court rejected the defendant's claims, opining 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 […]."[22]

III. Characteristics of Federal BIPA Cases Filed Between January 2015 and September 2024

To gain insight into the characteristics of BIPA litigation, a team of reviewers extracted information for 909 BIPA cases filed between January 1, 2015, and September 1, 2024, in U.S. federal court from Lex Machina, LexisNexis's legal analytics platform.[23] The reviewers collected data on the type of biometric information at issue, the industry in which the alleged violation occurred, and whether the plaintiff was a worker or consumer. The resulting dataset provides information on several key characteristics of BIPA cases filed in federal court during this period.[24]

Biometric identifiers. The largest shares of federal BIPA cases involved the use of either fingerprints (52%) or face geometry (40%), followed by hand geometry (11%), voiceprint (7%), and iris scan (1%).[25] The prevalence of fingerprints and face geometry in BIPA cases is generally consistent with the widespread use of these two biometric identifiers across the globe.[26] One study analyzing biometric adoption found that, between 2004 and 2016, fingerprints and face geometry constituted more than half of all biometric identifiers,[27] and, in 2024, fingerprints accounted for the largest share of all biometric identifiers globally.[28] Although iris scans accounted for 13% of

---

[20] Rosenbach v. Six Flags Entm't Corp., 2019 IL 123186, ¶¶ 5-6, 8.

[21] *Id.*, ¶ 12.

[22] *Id.*, ¶ 40.

[23] As part of LexisNexis, Lex Machina provides legal analytics for companies and legal professionals and contains detailed court dockets for BIPA matters filed in U.S. federal courts. *See Lex Machina*, LexisNexis https://lexmachina.com. While any person aggrieved by a BIPA violation can file their matter in a U.S. state court or federal court, for the purposes of our analysis we focus on litigation filed in U.S. federal court because information is not systematically available for all BIPA matters filed in U.S. state courts. *See* Biometric Information Privacy Act, 740 ILCS 14 (2008), Section 20. We also focus on U.S. federal court since BIPA class actions are typically brought in state court, subsequently removed from state to federal court by the defendant—particularly class actions under the *Class Action Fairness Act*—and dismissed based on lack of Article III standing. *See* Sojung Lee, *Give Up Your Face, and a Leg to Stand on Too: Biometric Privacy Violations and Article III Standing*, 90 The George Washington Law Review (2022), pp. 798-799; Mary Fletcher, *Preventing Gamesmanship: BIPA Class Action Litigation in the State and Federal Forums*, 67 Saint Louis University Law Journal (2023), pp. 399, 409.

[24] For ease of exposition, we refer to the federal BIPA class actions in our database as "BIPA cases" throughout this article.

[25] A single federal BIPA case can involve more than one type of biometric identifier, and all at-issue biometric identifiers are included in the percentages. For example, if a case involves both fingerprint and face geometry, the case would be included in the share in both categories.

[26] *Biometric Technology Market Size, Share & Trends Analysis Report By Component, By Offering, By Authentication Type, By Application, By End-use, By Region, And Segment Forecasts, 2023 - 2030*, Grand View Research, https://www.grandviewresearch.com/industry-analysis/biometrics-industry.

[27] Rachel German & K. Suzanne Barber, *Current Biometric Adoption and Trends*, Center for Identity at The University of Texas at Austin (Sept. 2017), https://identity.utexas.edu/sites/default/files/2020-09/Current%20Biometric%20Adoption%20and%20Trends.pdf, p. 5.

[28] Shivani Zoting, *Biometrics Market Size, Share, and Trends 2025 to 2034*, Precedence Research (Feb. 7, 2025), https://www.precedenceresearch.com/biometrics-market.

biometrics used for authentication between 2004 and 2016,[29] and their adoption has increased over time,[30] only 1% of federal BIPA cases involved this biometric identifier. This finding is likely due to the fact that iris scans are disproportionately used in government settings (e.g., immigration control and law enforcement), and state and local government agencies are not covered by BIPA.[31]

Industry. Biometric technologies have been adopted in a wide range of industries for a variety of uses. Even traditional industries—such as automotive, retail services, and financial services—have adopted these technologies.[32] Manufacturers, for example, have adopted biometric technologies for automating access at facilities instead of providing employees with individual key fobs, for streamlining employee timekeeping, and for integrating biometric systems into heavy machinery to increase safety instead of relying on foreman oversight.[33] Government agencies routinely deploy iris scanners for airport screening and facial recognition software for law enforcement.[34] The retail sector often uses fingerprint scanners for more efficient administrative employee timekeeping and payroll.[35]

As shown in **Figure 2**, the industry sectors associated with BIPA cases filed in federal court reflect the widespread adoption of biometric technologies across many sectors in the U.S.[36] Two industries—manufacturing and retail trade—account for 44% of all BIPA matters. These two industries, along with the information and transportation and warehousing industries, account for approximately two-thirds of all federal BIPA cases from January 1, 2015, through September 1, 2024. The remaining BIPA cases are associated with a variety of service industries, including hospitality, healthcare, finance, and the arts, among others.

---

[29] German & Barber, Center for Identity at The University of Texas at Austin, *supra* note 27, p. 5.

[30] Zoting, Precedence Research, *supra* note 28.

[31] Biometric Information Privacy Act, 740 ILCS 14 (2008), Section 10. *See also Types of Biometrics: Eye: Iris—Use Cases*, Biometrics Institute, https://www.biometricsinstitute.org/types-of-biometrics-eye-iris-use-cases/; *Features of Iris Recognition*, NEC (Sept. 22, 2021), https://www.nec.com/en/global/solutions/biometrics/iris/index.html.

[32] *9 Industries Biometrics Technology Could Transform*, CB Insights (Dec. 12, 2019), https://www.cbinsights.com/research/biometrics-transforming-industries/.

[33] *The Role of Biometrics in the Manufacturing Industry*, TrueID (June 24, 2023), https://www.trueid.in/blog/the-role-of-biometrics-in-the-manufacturing-industry/.

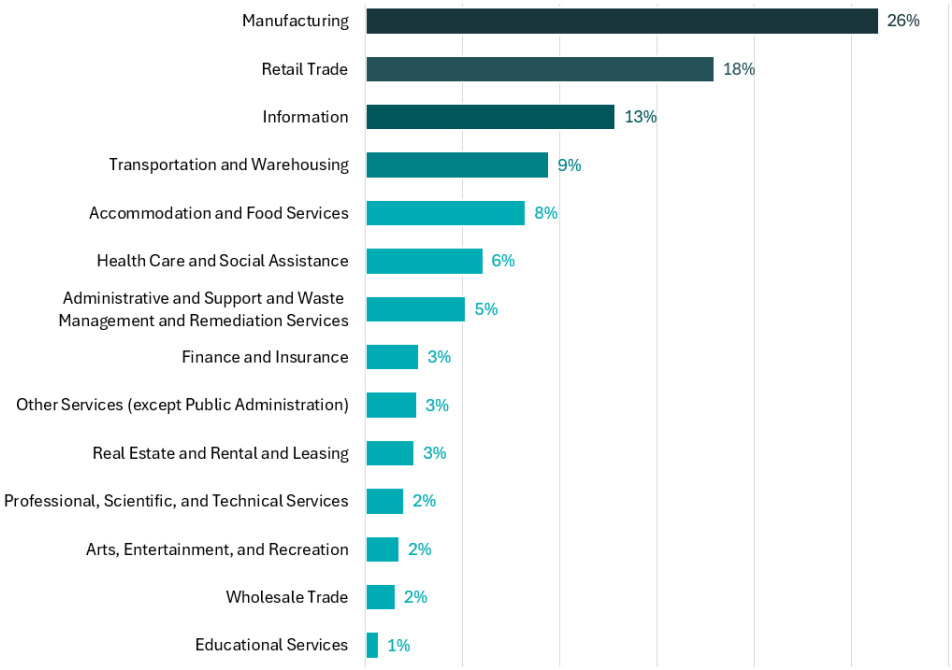
[34] *Facial Recognition Services: Federal Law Enforcement Agencies Should Take Actions to Implement Training, and Policies for Civil Liberties*, U.S. Government Accountability Office (Sept. 12, 2023), https://www.gao.gov/products/gao-23-105607. *See also,* Biometrics Institute, *supra* note 31.

[35] Chris Neely, *Why Adding Biometrics to Employee Time Clocks Makes a Lot of 'Cents'*, HID (Nov. 4, 2024), https://blog.hidglobal.com/why-adding-biometrics-employee-time-clocks-makes-lot-cents.

[36] We categorized each of the 909 BIPA matters filed in U.S. federal courts based on the defendant's industry according to the North American Industry Classification System (NAICS) manual provided by the United States Office of Management and Budget. For example, if the plaintiffs' biometric information was used while virtually trying beauty products through a defendant's retail store website, the case is assigned the two-digit NAICS code 44-45 Retail Trade and the four-digit NAICS code 4561 Health and Personal Care Retailers. In addition, BIPA lawsuits can involve more than one defendant (e.g., an employer where the plaintiff scans her fingerprints to "clock in" and "clock out," but also a biometric technology provider). In these circumstances, we use the plaintiff's experience—or their day-to-day interaction with their biometric identifiers—to assign one NAICS code for each BIPA matter (i.e., we assign NAICS codes based on the plaintiff's experience with their employer where they "clock in" and "clock out" instead of assigning NAICS codes based on the biometric technology provider). *See North American Industry Classification System*, Office of Management and Budget (2022), https://www.census.gov/naics/reference_files_tools/2022_NAICS_Manual.pdf.

Figure 2

Industries Associated with BIPA Cases

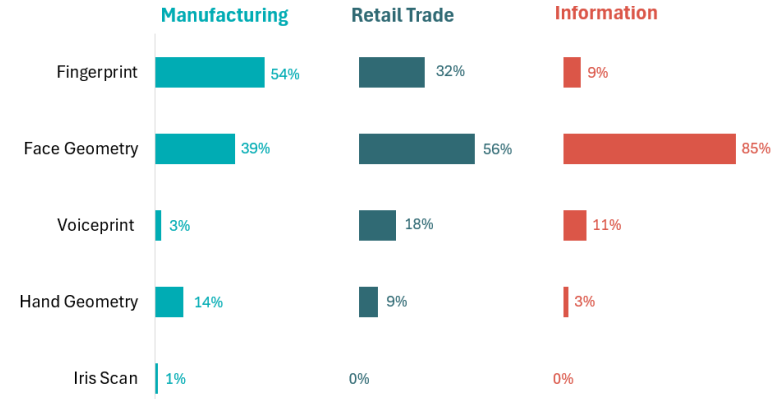


Within a given industry sector, BIPA cases cover a range of entities, again reflecting the widespread adoption and different uses of biometric technologies in the U.S. economy. Of the 240 BIPA cases involving defendants in the manufacturing sector, 100 are associated with the computer and peripheral equipment manufacturing industry, the majority of which were cases brought against biometric technology providers. The remainder of cases in the manufacturing sector are spread over 49 different four-digit North American Industry Classification System (NAICS) codes, covering manufacturing of a wide range of products, from baked goods to aerospace parts.

The type of biometric identifier at issue also varies across BIPA cases in different industries. As shown in **Figure 3**, the use of fingerprints is the most common type of identifier at issue in BIPA manufacturing cases. By contrast, most cases involving firms in retail trade and the vast majority of cases involving firms in the information industry included allegations related to the use of face geometry. The use of voiceprints accounts for 18% and 11% of BIPA cases involving firms in retail trade and information industries, respectively, but only 3% of cases in the manufacturing sector.

Figure 3

Biometric Identifier at Issue in BIPA Cases: Manufacturing, Retail Trade, and Information Industries[37]



[37] The total percentage of manufacturing, retail trade or information may be larger than 100% because some cases involve more than one type of biometric identifier.

In the consumer context, people can choose on a case-by-case basis whether they would like to enable the biometric features. However, in the employment context, workers' options for opting out of the use of biometric technologies may be more limited, which may increase the likelihood that the use of such technologies is challenged in litigation.

Type of plaintiff. We also classified plaintiffs in BIPA cases into two categories based on whether they are workers or consumers. In the employment context, most BIPA matters involve, for example, plaintiffs providing biometric identifiers to authenticate and "clock-in" and "clock-out" of an employer's timekeeping and payroll system. By contrast, cases involving consumers frequently relate to their use of biometric identifier(s) to access a wide range of services, such as secure access to apps and accounts or virtual eyewear and cosmetic applications.[38]

Plaintiffs were workers in 58% of BIPA cases filed in federal court between January 1, 2015, and September 1, 2024, and consumer plaintiffs comprised the remaining 42% of cases. The higher share of BIPA cases that are filed in the employment context may be rooted in differences in individual preferences over the collection and use of different types of biometric information and in different settings. This is borne out by consumer surveys and academic research. For example, approximately half of Americans are willing to provide their biometrics online to enroll, authenticate, and streamline login to access financial services, while only 21% of Americans are willing to do the same for retail functionality.[39] Similarly, published research shows that U.S. consumers are more comfortable providing fingerprints than eye scans.[40] A survey of consumers from eight countries indicates that more than half of respondents use fingerprint or face scan to unlock their mobile devices.[41] In some cases, consumers use these biometric technologies more than 100 times a day.[42] In the consumer context, people can choose on a case-by-case basis whether they would like to enable the biometric features. However, in the employment context, workers' options for opting out of the use of biometric technologies may be more limited, which may increase the likelihood that the use of such technologies is challenged in litigation.

The type of biometric identifiers at issue also differs between worker- and consumer-plaintiff BIPA cases. As shown in **Figure 4**, in the employment context, 83% of BIPA cases involved the use of fingerprints, followed by the use of hand geometry (16%). By contrast, 84% of consumer-plaintiff BIPA cases involved the use of face geometry technology, followed by the use of voiceprints (13%). These differences likely reflect differences in the type of biometric technologies that are typically used in the context of consumer products and the workplace.

---

[38] BIPA lawsuits can involve more than one defendant (e.g., an employer where plaintiff scans her fingerprints to "clock in" and "clock out," but also a biometric technology provider). In these circumstances, we use plaintiff's experience—or their day-to-day interaction with their biometric identifiers—to assign each BIPA matter as an employment or consumer technology matter (i.e., we assign plaintiff's experience with their employer where they "clock in" and "clock out" as an employment matter instead of consumer technology matter, even though defendant could also be a biometric technology provider).

[39] *Remote ID Verification: Bringing Confidence to Biometric Systems*, Fido Alliance (2024), https://fidoalliance.org/wp-content/uploads/2024/05/Consumer-Insights-2024-May292024.pdf, slide 4.

[40] Samantha Chavanic, *Research Finds US Adults Have Context-Specific Views on Biometric Technology Use*, Penn State University (Nov. 22, 2021), https://www.psu.edu/news/engineering/story/research-finds-us-adults-have-context-specific-views-biometric-technology-use.

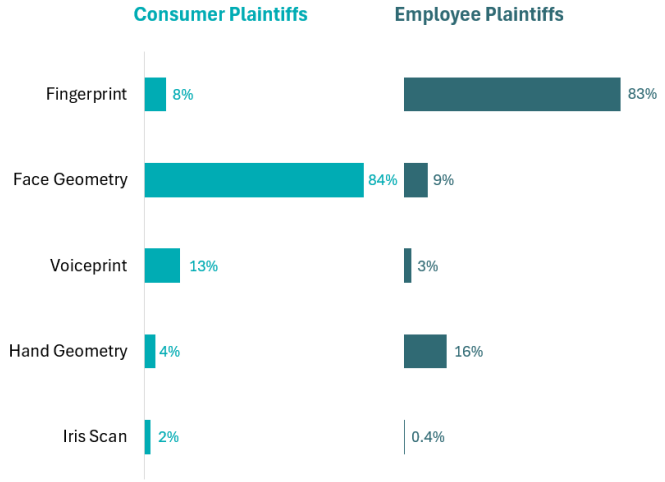
[41] *Over Half of Consumers Use Biometrics to Secure Mobile Devices*, Security Magazine (Oct. 26, 2022), https://www.securitymagazine.com/articles/98532-over-half-of-consumers-use-biometrics-to-secure-mobile-devices.

[42] *Apple Platform Security*, Apple (Dec. 19, 2024), https://support.apple.com/en-ca/guide/security/sec067eb0c9e/web.

The high share and number of BIPA cases with employee plaintiffs in the manufacturing and transportation and warehousing industries highlights the potential tradeoffs that employers may face when deploying biometric technologies in the workplace—timekeeping and payroll efficiencies versus the risk of BIPA litigation.

Figure 4

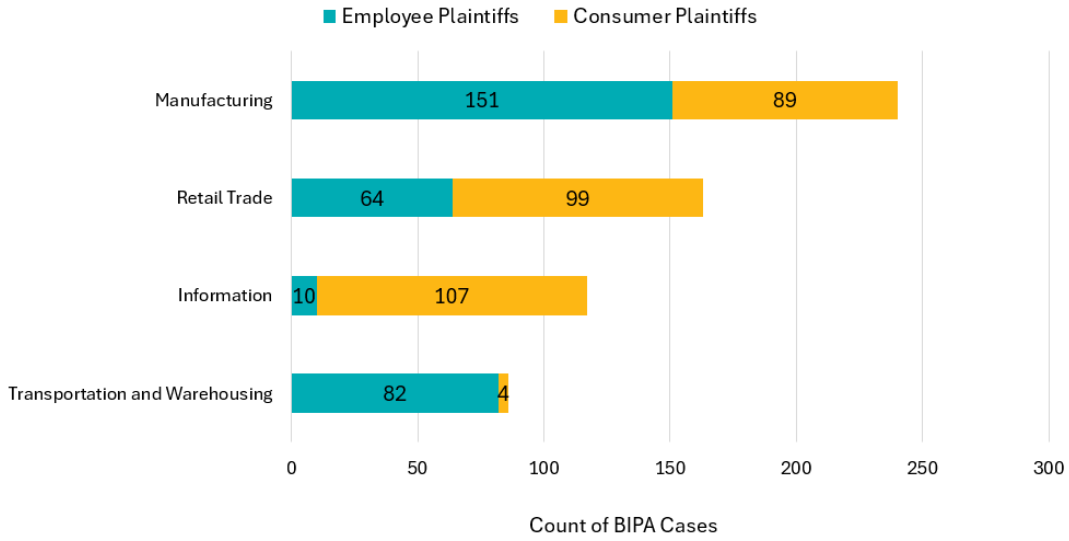
BIPA Cases by Plaintiff Type and Biometric Identifier[43]



BIPA cases with worker plaintiffs are more common in some industries than others. **Figure 5** shows the breakdown in plaintiff type for the four industries with the highest number of BIPA cases filed in federal court from January 1, 2015, to September 1, 2024: manufacturing, retail trade, information, and transportation and warehousing. While cases with employee plaintiffs account for the majority of BIPA cases in the manufacturing and transportation and warehousing industries, consumer plaintiffs account for the majority of BIPA cases in the retail trade and information industry sectors. The high share and number of BIPA cases with employee plaintiffs in the manufacturing and transportation and warehousing industries highlights the potential tradeoffs that employers may face when deploying biometric technologies in the workplace—timekeeping and payroll efficiencies versus the risk of BIPA litigation.

Figure 5

BIPA Cases by Plaintiff Type in Four Industries with the Highest BIPA Case Counts



[43] The total percentage of consumer plaintiffs or employee plaintiffs may be larger than 100% because some cases involve more than one type of biometric identifier.

IV. Trends in Federal BIPA Litigation Over Time

The surge in BIPA litigation activity in the past five years is shaping private entities' approaches to biometric privacy compliance and litigation across the country.

The BIPA litigation landscape has continued to evolve since its enactment in October 2008. The surge in BIPA litigation activity in the past five years is shaping private entities' approaches to biometric privacy compliance and litigation across the country. As the adoption of biometric identifiers continues to increase—with accelerated growth predicted over the next decade[44]—the legal landscape is also evolving, with key court rulings in BIPA cases and cases involving other state biometric privacy laws with similar requirements to BIPA (e.g., the Texas *Capture or Use of Biometric Identifier Act*).[45]

As described above, the number of BIPA cases filed in federal courts increased dramatically following the January 2019 Illinois Supreme Court's ruling in *Rosenbach.* Another increase in BIPA litigation activity followed the 2022 verdict in *Rogers v. BNSF Railway Company,* the first-ever BIPA case tried to a verdict.[46] In *Rogers*, plaintiff Richard Rogers, a truck driver, was required to register and scan his fingerprints in a biometrically enabled auto-gate system to access BNSF railyards.[47] Rogers alleged that BNSF failed to provide notice and obtain written consent before collecting biometric information, and in October 2022, a federal jury found that BNSF committed 45,600 violations—one for every individual who was required to register their fingerprints at BNSF facilities.[48] The jury ruled in favor of the plaintiff class, awarding damages of $228 million in total, $5,000 for each violation.[49]

[T]he number of BIPA cases filed in federal courts increased dramatically following the January 2019 Illinois Supreme Court's ruling in Rosenbach.

Concerns over the massive size of potential financial liabilities post-*Rogers* were a central issue in a subsequent decision by the Illinois Supreme Court in February 2023. Responding to a certified question from the U.S. Court of Appeals for the Seventh Circuit, the Illinois Supreme Court held in *Cothron v. White Castle System, Inc.* that "a separate claim accrues under the Act each time a private entity scans or transmits an individual's biometric identifier or information."[50] As manager of a White Castle restaurant, plaintiff Latrina Cothron was required to scan her fingerprints to access pay stubs and computers, and alleged that a new claim accrued each time she was required to scan her fingerprints.[51] The Illinois Supreme Court agreed.[52] Concerning damages accrual, the defendant cautioned the court that allowing for separate claims for each scan or transmission would result in "astronomical" damage awards.[53] In the context of *Cothron*, if the plaintiff had been allowed to bring her claims on behalf of the 9,500 current and former White Castle employees, class-wide damages in her action could have been in the order of $17 billion.[54]

---

[44] Oloid, *supra* note no53vv.

[45] *Meet CUBI—What Companies Need to Know About Texas' Biometric Privacy Law*, Blank Rome (Oct. 5, 2020), https://www.blankrome.com/publications/meet-cubi-what-companies-need-know-about-texas-biometric-privacy-law.

[46] Kristin Bryan, *BREAKING: Plaintiff Prevails In First BIPA Class Action Jury Trial*, Privacy World (Oct. 12, 2022), https://www.privacyworld.blog/2022/10/breaking-plaintiff-prevails-in-first-bipa-class-action-jury-trial/.

[47] Rogers v. BNSF Ry. Co., 680 F. Supp. 3d 1027 (N.D. Ill. June 30, 2023).

[48] Second Amended Class Action Complaint, Rogers v. BNSF Ry. Co. (Sept. 10, 2021) (No. 19-CV-08083), ¶ ¶ 31-33. *See also, Rogers*, F. Supp. 3d, pp. 1032-33.

[49] *Rogers*, F. Supp. 3d, p. 1032.

[50] Cothron v. White Castle System, Inc., 2023 IL 128004 , ¶ 1.

[51] *Id.*, ¶ ¶ 4, 7.

[52] *Id.*, ¶ 1.

[53] *Id.*, ¶ 40.

[54] *Id.*, ¶ 40.

During its consideration of the significant liabilities in *Cothron*, the Illinois Supreme Court cited language that appeared "to make damages discretionary rather than mandatory" since,[55] under BIPA, a "prevailing party *may* recover" damages (emphasis added).[56] The court also reiterated that "there is no language in the Act […] to authorize a damages award that would result in the financial destruction of a business."[57] This decision was important for the retrial of *Rogers*, where the previous $228 million damages award was vacated.[58] While the ruling provided some relief for BIPA defendants, BNSF ultimately agreed to a $75 million settlement.[59]

In August 2024, in response to the *Cothron* decision, Illinois Governor J.B. Pritzker signed into law an amendment to BIPA, which provided that "a private entity that more than once collects or discloses a person's biometric identifier or biometric information from the same person in violation of the Act has committed a single violation for which the aggrieved person is entitled to, at most, one recovery."[60] At the time the amendment was passed, there were questions about whether this change to BIPA, which limited businesses' exposure, could be applied retroactively to pending cases. These questions were addressed by subsequent rulings in Illinois federal courts.

- On November 13, 2024, U.S. District Judge Elaine Bucklo held in *Gregg v. Central Transport LLC* that the amendment did apply retroactively to claims filed before August 2024, noting that the BIPA amendments "clarified" the legislature's intent, and therefore, the amendments "must be applied as if [they] were clear from the date of the BIPA's enactment."[61]
- On November 22, 2024, U.S. District Judge Georgia Alexakis came to the opposite conclusion in *Schwartz v. Supply Network, Inc.*, ruling that "[b]ecause the amendment to the Act is substantive, and the Illinois legislature did not expressly make it retroactive, Illinois law compels that the amendment be applied prospectively, not retroactively."[62]
- On January 21, 2025, in *Giles v. Sabert Corporation*, U.S. District Judge Sara Ellis agreed with Judge Alexakis reasoning in *Schwartz*, noting that "BIPA was unambiguous, with the language of [the amendment] supporting that it effected a change, not a clarification, in the law."[63]
- On March 21, 2025, Judge Bucklo vacated her prior finding in *Gregg* that the law did not apply retroactively, "[b]ecause upon further consideration, I am persuaded that the better interpretation of the amendment is that it effected a change in the law."[64] In her reconsideration, Judge Bucklo noted other courts have reached a similar conclusion.[65]

---

[55] *Id.*, ¶ 42.

[56] Biometric Information Privacy Act, 740 ILCS 14 (2008), Section 20.

[57] *Cothron*, 2023 IL 128004, ¶ 42.

[58] *Rogers*, F. Supp. 3d, pp. 1032, 1040–42.

[59] Lauraann Wood, *BNSF's $75M BIPA Deal With Truckers Nears Final OK*, Law360 (June 17, 2024), https://www.law360.com/articles/1848754/bnsf-s-75m-bipa-deal-with-truckers-nears-final-ok.

[60] Public Act 103-0769, 740 ILCS 14 §§ 10, 20 (Aug. 2, 2024) (amending Biometric Information Privacy Act, 740 ILCS 14 (2008)). *See also,* Michael McCutcheon, et al., *United States: The Conflicting Decisions of Federal Courts in Illinois Leave the Retroactivity of BIPA's Amendment in Flux*, Baker McKenzie (Dec. 3, 2024), https://insightplus.bakermckenzie.com/bm/dispute-resolution/united-states-federal-court-rules-that-amendments-to-illinois-bipa-statute-apply-retroactively-to-bar-the-ability-of-plaintiffs-to-recover-damages-for-multiple-violations.

[61] Gregg v. Central Transport LLC, 2024 U.S. Dist. LEXIS 206003 (N.D. Ill. Nov. 13, 2024), p. 8.

[62] Schwartz v. Supply Network Inc., 2024 U.S. Dist. LEXIS 213002, 2024 WL 4871408 (N.D. Ill. Nov. 22, 2024), p. 12.

[63] Giles v. Sabert Corp., 2025 U.S. Dist. LEXIS 12888, 2025 WL 274326 (N.D. Ill. Jan. 21, 2025), pp. 8-9.

[64] Gregg v. Central Transport LLC, 2025 U.S. Dist. LEXIS 53731, 2025 WL 907540 (N.D. Ill. Mar. 21, 2025), p. 2.

[65] *Id.*

The significant size of BIPA class action settlements in recent years underscores the extent of potential liabilities that private entities may face and the importance of ensuring that they stay in compliance.

The significant size of BIPA class action settlements in recent years underscores the extent of potential liabilities that private entities may face and the importance of ensuring that they stay in compliance. For example:

- TikTok settled a class action alleging that it had violated BIPA by collecting users' facial geometry without their consent for $92 million in 2022;[66]
- Bumble and Badoo reached a $40 million settlement with a class of users in Illinois alleging that the dating apps unlawfully collected facial geometry scans from photos uploaded by users to the apps;[67]
- Kronos Inc., a provider of biometric-based timekeeping solutions, settled a class action brought by employees who scanned their fingerprints on Kronos-brand timeclocks at their jobs in Illinois for $15.3 million in 2022;[68] and
- As discussed above, BNSF settled a class action involving the collection of fingerprint scans from drivers using automated gate systems at company facilities for $75 million in 2024.[69]

The litigation against Kronos Inc. highlights the potential liability not only of employers deploying biometric technology at their premises for timekeeping purposes, but also of biometric technology vendors themselves. Some courts have held that such third-party entities can be held liable under BIPA even if they do not directly interface with individuals providing the biometric data.[70] However, judicial decisions in other cases have suggested that the scope of third-party liability under BIPA may be more limited. For example, in *Jones v. Microsoft Corporation*, the court ruled that BIPA does not apply to a vendor to the third party that "merely" provided the biometric data collection technology.[71] Courts have also dismissed cases brought against companies that did not actively obtain biometric data but served only as a back-end cloud services provider.[72]

Trends in the at-issue biometric identifiers over time. While the majority of BIPA cases filed in federal court involve the use of fingerprints and face geometry, there have been notable changes over time, as shown in **Figure 6**. First, BIPA cases involving voiceprints have been increasing since 2016, reflecting an increasing number of cases involving interactive chatbots, call centers, and personal AI assistants.[73] This trend mirrors the growing adoption of voice assistant technologies by consumers.[74] Second, between 2020 and 2022, there was a large decline in the number of cases involving fingerprints and a corresponding increase in cases involving face geometry and

---

[66] *Judge Approves $92 Million TikTok Settlement*, Hunton (Aug. 9, 2022), https://www.hunton.com/privacy-and-information-security-law/judge-approves-92-million-tiktok-settlement.

[67] *$40M Bumble, Badoo BIPA Class Action Settlement*, Top Class Action (Aug. 29, 2024), https://topclassactions.com/lawsuit-settlements/closed-settlements/40m-bumble-badoo-bipa-class-action-settlement/.

[68] Lauraann Wood, *Kronos' $15.3M Biometric Privacy Deal Gets Early OK*, Law360 (Feb. 22, 2022), https://www.law360.com/articles/1467242.

[69] Mike Scarcella, *BNSF Railway to Pay $75 mln to Resolve Biometric Privacy Class-Action*, Reuters (Feb. 27, 2024), https://www.reuters.com/legal/litigation/bnsf-railway-pay-75-mln-resolve-biometric-privacy-class-action-2024-02-27/.

[70] *See, for example*, Johnson v. NCR Corp., 2023 U.S. Dist. LEXIS 19327, 2023 WL 1779774 (N.D. Ill. Feb. 6, 2023), p. 5. *See also,* Rivera v. Amazon Web Servs., 2023 U.S. Dist. LEXIS 129517, 2023 WL 4761481 (W.D. Wash. July 26, 2023), pp. 6-9.

[71] Jones v. Microsoft Corp., 649 F. Supp. 3d 679 (N.D. Ill. 2023), p. 684.

[72] *See, for example*, Clark v. Microsoft Corp., 688 F. Supp. 3d 743 (N.D. Ill. Aug. 21, 2023), pp. 747-748.

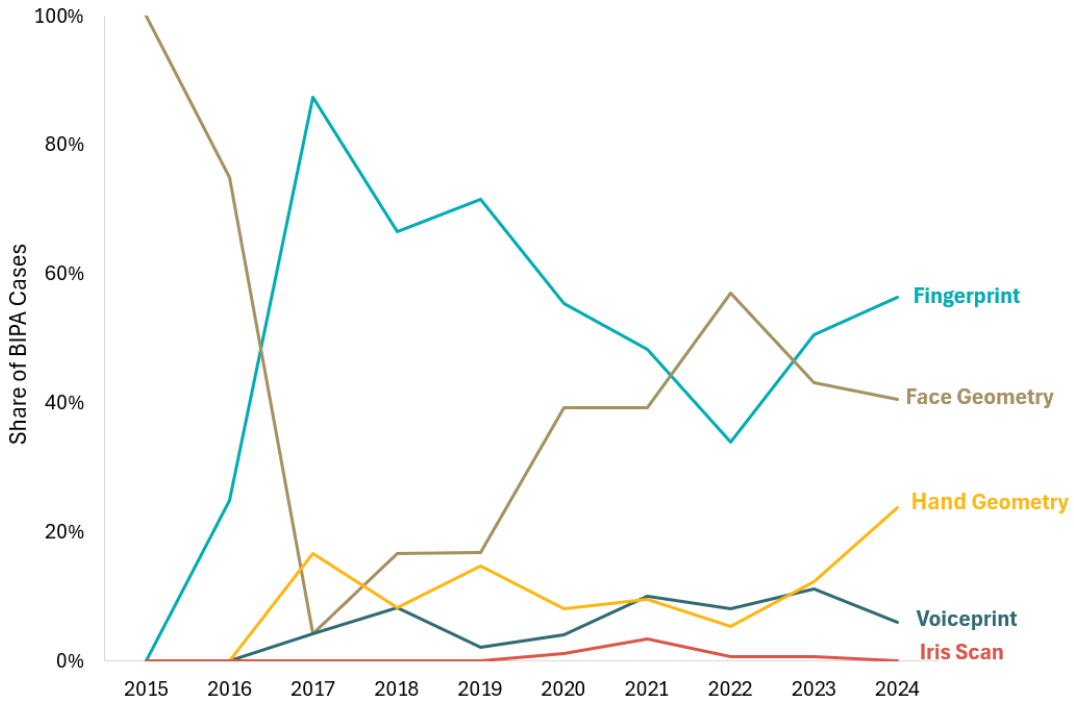
[73] *See, for example,* Class Action Complaint, Flores v. Amazon Inc., (W.D. Wash. June 10, 2021) (No. 1:21-cv-04064). *See also,* Class Action Complaint, Duncan v. Five9, Inc., (Ill. Cir. September 15, 2023) (No. 1:23-cv-13779); Class Action Complaint, Batchuluun v. Wingstop Inc., (N.D. Ill. Mar. 20, 2024) (No. 1:24-cv-02302).

[74] Chris Keating, *Data Drop: Gen Z Leading Voice Assistant Growth*, EMARKETER (Oct. 19, 2023), https://www.emarketer.com/content/data-drop-gen-z-leading-voice-assistant-growth.

voiceprints. This pattern coincides with the COVID-19 pandemic, a period during which people may have been more likely to use contactless biometric technologies. For example, the number of BIPA cases involving the use of e-proctoring technologies (hybrid educational tools used to supervise exams by using students' face geometry, iris scan, and voiceprint) rose from one case filed in 2020 to eight cases filed in 2021. This rise in cases involving e-proctoring technologies can be attributed to the rapid adoption of these technologies by universities and other educational entities to monitor online exams for remote learning during the COVID-19 pandemic and beyond.[75]

Figure 6

BIPA Cases by Biometric Identifier at Issue[76]



Declines in cases involving workers during COVID-19. While the trends in employment and consumer technology matters largely mirror the overall post-*Rosenbach* landscape, employment-related matters experienced a downturn after 2020 and increased again in 2023, as shown in **Figure 7**. The global shift to remote working and to touchless technologies to prevent the spread of COVID-19 likely explain the decrease in employment-related matters,[77] as the majority of cases filed on behalf of workers involve fingerprint biometric identifiers. (See **Figure 4**.)

---

[75] Faten F. Kharbat & Ajayeb S. Abu Daabes, *E-Proctored Exams During the COVID-19 Pandemic: A Close Understanding*, 26 Education and Information Technologies (2021). *See also,* Kazma Chaudhry, et al., *'It's Not That I Want to See the Student's Bedroom . . .': Instructor Perceptions of e-Proctoring Software*, European Symposium on Usable Security (2023).

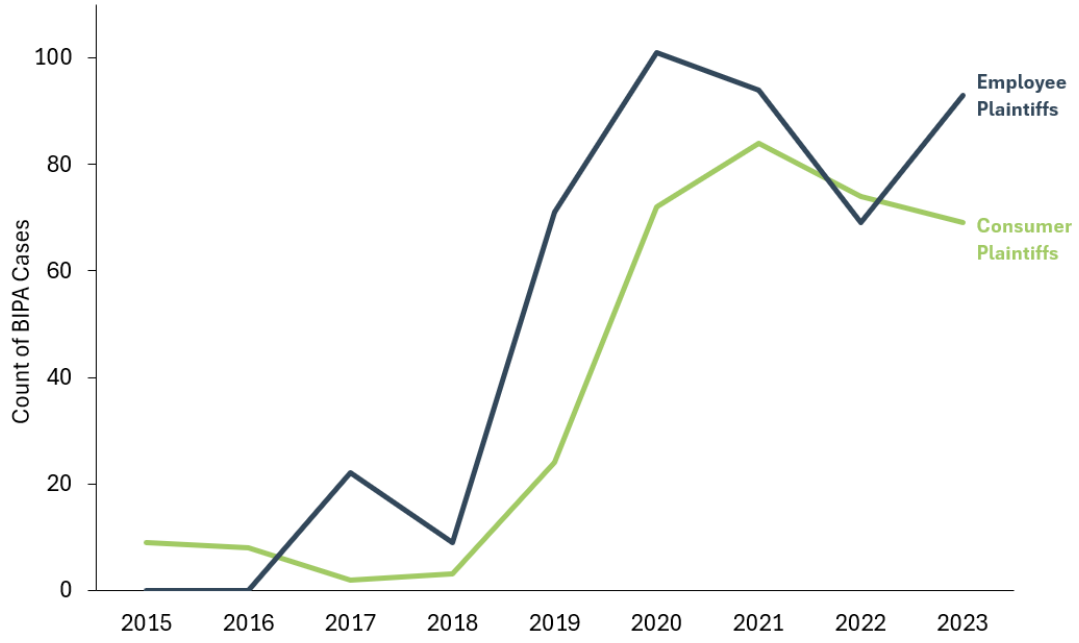
[76] The total percentage of cases in a year may be larger than 100% because some cases involve more than one type of biometric identifier.

[77] *Improving Worksite Health Screening, Security and Workforce Management*, Digital, https://www.digitalsupercluster.ca/impact-story/improving-worksite-health-screening-security-and-workforce-management/. *See also,* Yuheng Guo, *Impact on Biometric Identification Systems of COVID-19*, Scientific Programming (2021).

Regulatory agencies—including the FTC—are also starting to investigate the collection and use of biometric information. In May 2023, the FTC released a policy statement on the use of biometric information and related technologies, and issued a warning on their use due to consumer privacy, data security, and bias and discrimination concerns.

Figure 7

Trends in BIPA Cases by Plaintiff Type



V. Future Developments

The August 2024 amendment to BIPA effectively overturned the Illinois Supreme Court per-scan damages holding in *Cothron* by expressly stipulating that repeated collection of the same biometric data without consent is deemed a single, collective violation.[78] It remains to be seen whether and how the limits on damages by the 2024 amendment will affect the numbers or the type of BIPA litigation filings going forward. Although the amendment provides some potential relief to companies against "annihilative liability,"[79] statutory damages per individual for BIPA violations remain substantial, and outcomes from BIPA-related matters are continuing to shape the way biometric cases are litigated in the U.S.

Beyond BIPA, other U.S. laws and agencies may also influence future trends in the regulation of—and litigation involving—biometric information. The State of Washington's inclusion of a private right of action for biometric-related violations—only the second state after Illinois to do so[80]—in its recently enacted *My Health My Data Act* could trigger another wave of biometric-related class action lawsuits.[81] Regulatory agencies—including the FTC—are also starting to investigate the collection and use of biometric information. In May 2023, the FTC released a policy statement on

---

[78] Public Act 103-0769, 740 ILCS 14 §§ 10, 20 (August 2, 2024). *See also Cothron*, 2023 IL 128004, ¶ 1.

[79] Michael B. Galibois, et al., *Illinois' BIPA Amendment Brings Relief to Private Entities*, Reed Smith, https://www.reedsmith.com/en/perspectives/2024/08/illinois-bipa-amendment-brings-relief-to-private-entities.

[80] Jennifer Quinn-Barabanov, et al., *BIPA 2.0? Washington's New Privacy Law Creates Private Litigation and AG Enforcement Risk for Businesses*, Steptoe, https://www.steptoe.com/en/news-publications/bipa-20-washingtons-new-privacy-law-creates-private-litigation-and-ag-enforcement-risk-for-businesses.html.

[81] Andreas T. Kaltsounis, et al., *Examining the Likely Impact of Washington's My Health, My Data Act on Class Action Litigation Involving Biometric Data*, BakerHostetler (Dec. 1, 2023), https://www.bakerdatacounsel.com/blogs/examining-the-likely-impact-of-washingtons-my-health-my-data-act-on-class-action-litigation-involving-biometric-data/. *See also,* Jacqueline Klosek, et al., *Washington's My Health My Data Act Comes Into Force—What You Need to Know, and Do*, Goodwin (Mar. 28, 2024), https://www.goodwinlaw.com/en/insights/publications/2024/03/alerts-technology-hltc-my-health-my-data-act-mhmda.

the use of biometric information and related technologies,[82] and issued a warning on their use due to consumer privacy, data security, and bias and discrimination concerns.[83]

Combined with the rapid proliferation of biometric technologies, the changing legal landscape has created significant shifts in BIPA litigation trends and uncertainties for businesses that are considering, or have already adopted, these technologies. As the landscape of biometric privacy law—and in particular, BIPA—continues to evolve, biometric information stakeholders must stay up to date on its most recent developments and applicability to biometric information that they may be collecting or storing. ●

[82] U.S. Federal Trade Commission, *supra* note 7.

[83] *FTC Warns About Misuses of Biometric Information and Harm to Consumers*, U.S. Federal Trade Commission (May 18, 2023), https://www.ftc.gov/news-events/news/press-releases/2023/05/ftc-warns-about-misuses-biometric-information-harm-consumers.